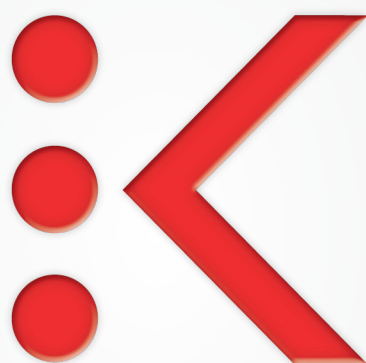




INDEPENDENCEKEY
Manuale dell'utente



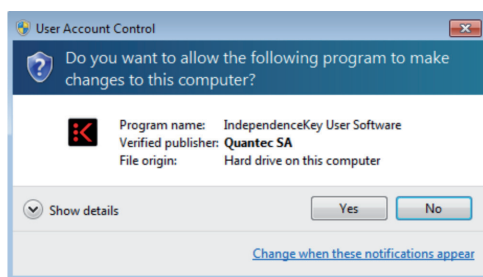
SOMMARIO

Installazione e inizializzazione del prodotto	04
Utilizzo di IndependenceKey per la sicurezza dei propri dati	06
Impostazioni iniziali	07
Criptare, aprire, modificare e decriptare un file	08
• Criptare una directory	09
QDisk. Creare un disco criptato	10
Cloud storage sicuro con IndependenceKey	12
Associazione con altri utenti	14
• Associazione remota	14
• Associazione fisica	16
Condivisione protetta delle informazioni	18
Utilizzo della porta USB host	20
• Eseguire un backup criptato su supporti esterni	20
Utilizzo del Security Cap	22
Utilizzo del Data Bank	27
Keylogger e Master Password	28
Programmi e autorizzazioni	29
Rimozione di IndependenceKey	31
Reset e migrazione	32
Supporto tecnico e assistenza	33
Troubleshooting	34
Appendice tecnica	38
Termini e condizioni per l'uso del software	40
Garanzia hardware	42
Norme sulla Privacy	44

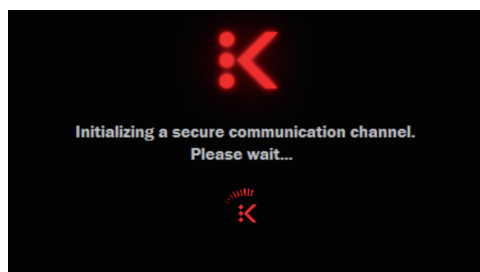
Installazione e inizializzazione del prodotto

Al primo utilizzo della tua IndependenceKey

- 01** Scaricare l'ultima versione del programma di setup dal sito di IndependenceKey al seguente indirizzo: <http://www.independencekey.com/download>
Per scaricare il software è necessario disporre del codice di autorizzazione che si trova stampato sul bugiardino all'interno della scatola di IndependenceKey o che vi è stato inviato via email.
- 02** Installare il software (sono necessari i diritti di amministratore della macchina), avendo cura di accettare eventuali richieste di autorizzazione da parte di programmi antivirus e firewall presenti sul computer oppure, a installazione avvenuta, creando le opportune regole e autorizzazioni in tali software. Il software di IndependenceKey è firmato digitalmente con certificato emesso da una Certification Authority. Ciò attesta la genuinità del software prodotto dalla Quantec SA. Per gli utenti dotati di sistema operativo Windows XP, prima di procedere si consiglia di leggere quanto riportato nell'appendice tecnica alla fine di questo manuale.



- 03** Una volta installato il software non occorre riavviare il computer, inserire il Security Cap nella propria IndependenceKey, quindi inserire IndependenceKey nel computer.
- 04** Windows ricercherà il driver già installato per associarlo al dispositivo. Questa operazione può durare uno o più minuti e viene eseguita solo una volta.
- 05** Comparirà la seguente schermata:



la quale indica che IndependenceKey è stata riconosciuta dal computer ed è in corso la cifratura del canale di comunicazione tra quest'ultimo ed il dispositivo.

ASPETTI TECNICI

Come è fatta IndependenceKey?

IndependenceKey è un dispositivo ad alta integrazione. È il più piccolo dispositivo crittografico portatile del mondo in grado di raggiungere e superare i 100 Mbps crittografici in tempo reale, dotato di una porta USB host (porta posteriore) e aperto a numerose applicazioni. È realizzato in lega di alluminio, con un trattamento superficiale specifico denominato PVD, totalmente atossico e nichel-free.

Cosa succede durante l'inizializzazione?

Sia all'interno di IndependenceKey, sia nel suo Security Cap è presente un chip crittografico di autenticazione della piattaforma di sicurezza TPM (Trusted Platform Module). Tramite tali chip e gli engine crittografici hardware ad alte prestazioni presenti nei due dispositivi, IndependenceKey e il suo Security Cap si associano indissolubilmente tra loro durante la fase di associazione, effettuando tutte le verifiche di anticloning necessarie, criptando il canale di comunicazione e memorizzando specifici segreti combinatori derivati dalla Master Password.

Dove viene memorizzata la Master Password?

La Master Password non viene mai memorizzata da nessuna parte, bensì vengono derivati da essa un insieme di segreti combinatori che in parte risiedono in IndependenceKey e in parte vengono memorizzati nel Security Cap. Nessuno dei due dispositivi, individualmente, è in grado di accedere al data base crittografato interno contenente tutti i dati di IndependenceKey. Solo chi conosce la Master Password può completare parte di tali segreti sbloccando uno dei due dispositivi.

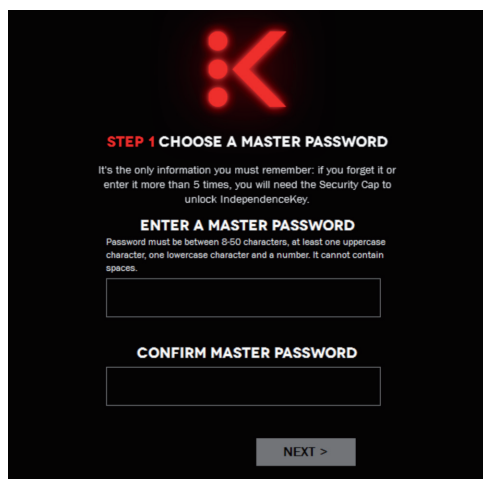
Se mi dimentico la Master Password?

È sufficiente unire IndependenceKey al proprio Security Cap e insieme, i due dispositivi possono sbloccare il data base crittografato perché dispongono dei segreti necessari. A questo punto è possibile cambiare a piacimento la propria Master Password.

Cos'è l'Alias?

L'Alias è l'impronta digitale del dispositivo. È un codice alfanumerico derivato dal Serial Number del chip di crittografia e dai segreti combinatori di fabbrica e non è né modificabile né clonabile. Una volta attivata la propria IndependenceKey, l'Alias accompagna l'utente durante tutta la vita del prodotto, anche in caso di upgrade a versioni successive.

06 Dopo alcuni secondi, verrà avviata la procedura di inizializzazione di IndependenceKey:



07 Seguire le istruzioni a video, inserendo una Master Password di minimo 8 caratteri contenenti almeno una lettera maiuscola, una minuscola e un numero (il software effettua le verifiche di congruità). Una volta confermata la Master Password, inserire il proprio Nickname che sarà utile per le successive associazioni con gli altri utenti.

Prendere nota dell'Alias della propria IndependenceKey che compare sotto il Nickname. **Tale codice è l'identificativo univoco del vostro prodotto, non può essere modificato né clonato.** È il codice che dovrete fornire agli altri utenti se volete associarvi tramite Internet (si veda il capitolo relativo all'associazione).

L'inizializzazione del prodotto deve essere eseguita solo una volta e richiede circa un minuto, il tempo necessario a entrambi i dispositivi per effettuare le verifiche di genuinità, anticloning, crittografare il canale di comunicazione e creare il data base principale che conterrà le chiavi crittografiche e i dati del Password Manager.

Nel riquadro a lato trovate una descrizione dettagliata di cosa avviene durante questa fase.

Al termine dell' inizializzazione, quando compare il messaggio di finalizzazione della procedura, togliere il Security Cap, anche lasciando la propria IndependenceKey inserita, e riportarlo in un luogo sicuro. IndependenceKey è pronta per essere utilizzata.

IndependenceKey non funziona se il Security Cap è inserito in quanto, quest'ultimo, è il dispositivo di backup e di sicurezza che va custodito in un luogo sicuro separato dalla propria IndependenceKey.

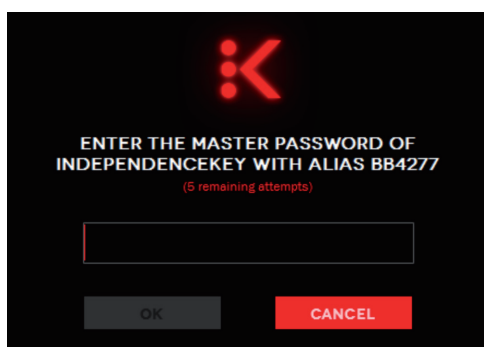


Utilizzo di IndependenceKey per la sicurezza dei propri dati

ASPETTI TECNICI

 Utilizzare IndependenceKey è facilissimo. Dopo averla inserita nel computer, prima di poterla usare bisogna sbloccarla. Questo può essere fatto in due modi: digitando la propria Master Password oppure inserendo il Security Cap con cui IndependenceKey è stata inizializzata. Questa seconda opzione è utile nel caso in cui, per qualche motivo, non si volesse digitare la propria Master Password.

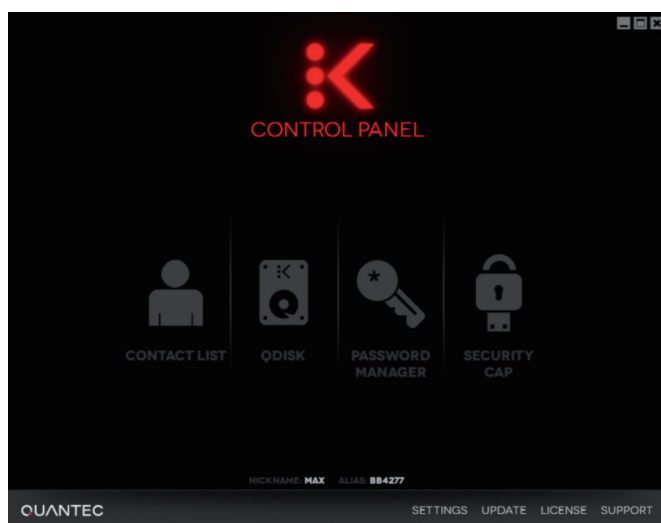
Installare il software (sono necessari i diritti di amministratore della macchina). Il software di IndependenceKey è firmato digitalmente con certificato emesso da una Certification Authority. Ciò attesta la genuinità del software prodotto dalla Quantec SA. Per gli utenti dotati di sistema operativo Windows XP, prima di procedere si consiglia di leggere quanto riportato nell'appendice tecnica alla fine di questo manuale.



Una volta che IndependenceKey è stata sbloccata, l'icona "K" in basso a destra nella system tray bar passa dallo stato "grigio" a "rosso". Se non è presente l'icona "K", occorre cliccare sul pulsante a forma di triangolo di Windows "▲" per espandere l'elenco delle icone.



Per aprire l'interfaccia principale basta un doppio click sull'icona a forma di "K".



Che cosa accade quando si inserisce IndependenceKey nel PC?

Ogni volta che IndependenceKey viene inserita nel computer avvia una nuova copia del proprio sistema operativo, sempre identica alla precedente, ovvero si avvia da una condizione nota e precostituita onde massimizzare i livelli di sicurezza del dispositivo.

Che sistema di crittografia utilizza IndependenceKey?

IndependenceKey è dotata di un engine crittografico accelerato via hardware in grado di raggiungere performances elevatissime con i più moderni standard crittografici tra i quali 3DES, AES256, AES-XTS, AES-GCM. Quantec ha sviluppato su tale engine, utilizzando l'AES, un engine crittografico a "finestre mobili" in grado di **adattarsi dinamicamente alla tipologia di dato da proteggere**, sia esso un file, un disco, o un flusso VoIP in streaming.

Come si crea la chiave di crittografia e dove si trova?

Le chiavi di crittografia vengono generate all'interno del dispositivo da un chip crittografico della piattaforma di sicurezza TPM, specificatamente dedicato a tale scopo. Queste chiavi sono uniche, universali e irripetibili ma, soprattutto, **tali chiavi crittografiche non lasciano mai il dispositivo stesso!** Questa è una caratteristica unica e molto importante di IndependenceKey.

Quali file posso proteggere? Di che dimensioni?

IndependenceKey non ha limitazioni sulla dimensione del file o delle informazioni che vengono criptate. Può operare su file, cartelle, dischi, così come su flussi VoIP e flussi A/V in streaming ad alta definizione in tempo reale.

A che velocità cripta il dispositivo?

IndependenceKey raggiunge e supera la velocità crittografica di 100 Mbps in tempo reale. Prossime versioni di IndependenceKey supereranno i 150-160 Mbps in tempo reale. Questi valori rendono IndependenceKey talmente efficace ed efficiente che, una volta inserita nel computer, non si nota la differenza con la normale operatività.

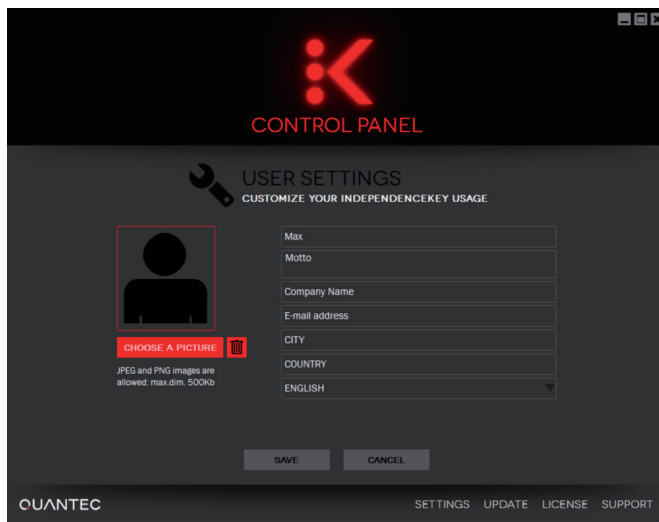
Come dialoga IndependenceKey con il computer?

Quando si inserisce IndependenceKey nel computer, il dispositivo si avvia e si attiva immediatamente la protezione del canale di comunicazione tra IndependenceKey e il computer. Ciò viene realizzato ricorrendo alle moderne tecniche di crittografia PKI (a chiave pubblica-privata). **Tutto il canale di comunicazione è crittografato**, anche lato computer, ma la cosa più importante è che IndependenceKey utilizza le chiavi crittografiche esclusivamente al proprio interno, senza mai farle uscire dal dispositivo stesso. Ciò eleva al massimo grado possibile i livelli di sicurezza. Inoltre, IndependenceKey è, per il computer in cui è inserita, una scheda di rete ad alta velocità (NIC interface). Ciò consentirà agli utenti di IndependenceKey di disporre di servizi avanzati di **VPN hardware**.

Impostazioni iniziali

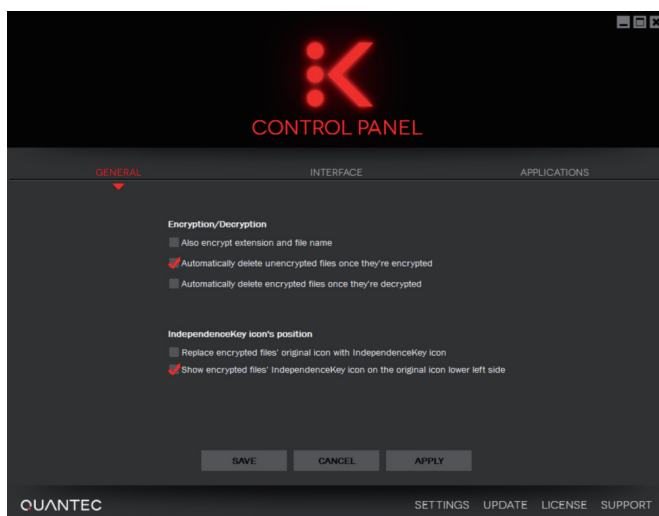
1

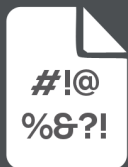
 Per modificare le impostazioni del programma relative al proprio profilo utente, lingua desiderata, etc.. cliccare su “Impostazioni” (“Settings”) e scegliere l’opzione “Modifica il tuo profilo” (“Edit your Profile”). Da qui è possibile cambiare la lingua dell’interfaccia scegliendo tra quelle disponibili.



Cliccando sull’opzione “Preferenze” (“Preferences”) si può regolare il comportamento di IndependenceKey secondo le proprie esigenze; per esempio effettuare il camuffamento (scrambling) dei nomi dei files quando essi vengono criptati, o mantenere una copia in chiaro dei file che si crittografano e gestire le altre opzioni disponibili.

IndependenceKey è in grado di eliminare per sempre e in automatico (auto-wiping) i file originali una volta crittografati. Data la sua capacità di lavorare direttamente sui file criptati senza lasciare traccia, si consiglia di operare con questa opzione sempre abilitata.

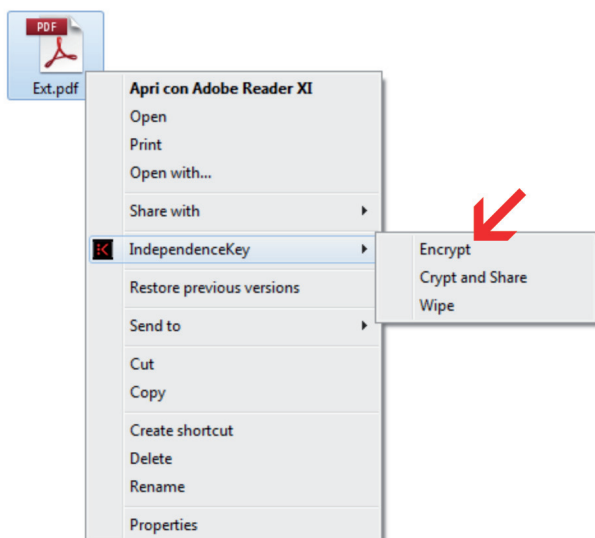




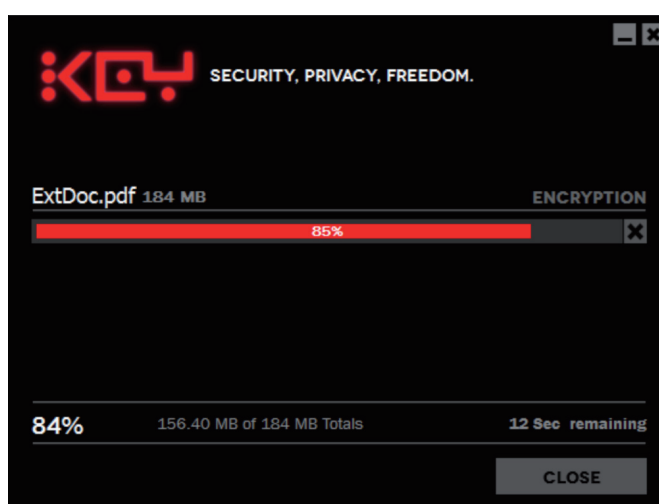
Criptare, aprire, modificare decriptare un file

CRIPTARE

È sufficiente cliccare con il pulsante destro del mouse sul file che si desidera criptare.



Quindi selezionare “IndependenceKey” -> “Encrypt”. Questa operazione consente di crittografare il file. L'avanzamento della procedura di crittografia può essere visionato tramite l'“Encryption Crate” dell'interfaccia di IndependenceKey (menù “Impostazioni” (“Settings”) -> “Encryption Crate”):



ASPETTI TECNICI

Quando si aprono i file criptati vengono fatte copie in chiaro?

Assolutamente NO! A differenza di tutti gli altri sistemi di crittografia software e non, **le applicazioni di alto livello** (Microsoft Word, Excel, Power Point e qualsiasi tipo di applicazione che può essere eseguita sul computer, compresi CAD/CAM, sistemi RAD, ambienti di authoring, etc..) **lavorano direttamente sui dati criptati; di questi file non viene mai creata una copia in chiaro da nessuna parte.** IndependenceKey decrittografa e crittografa in tempo reale i dati richiesti dall'applicazione rispettivamente quando quest'ultima legge e scrive nella memoria di storage del computer sul file criptato stesso. Tutto avviene in tempo reale nella memoria dell'applicazione.

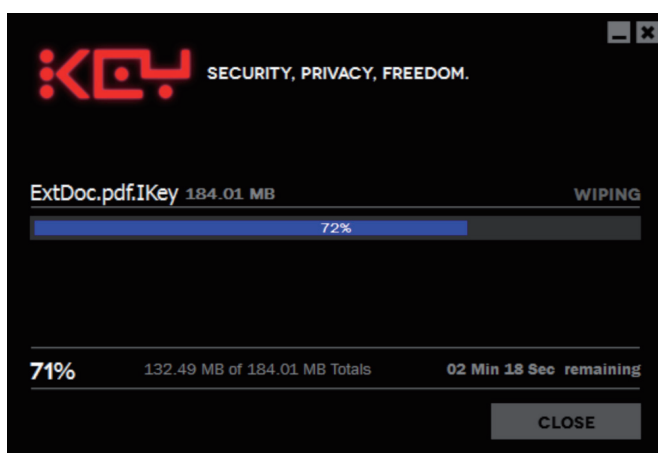
Perfino i file temporanei creati dalle applicazioni Microsoft Office vengono criptati e non ve ne è traccia sulla memoria di storage del computer. Ciò eleva in maniera rilevante i livelli di sicurezza, unitamente al fatto che i segreti necessari per accedere ai file criptati risiedono solo ed esclusivamente all'interno della propria IndependenceKey.

Come funziona?

IndependenceKey opera sotto il file system del sistema operativo, ovvero tra quest'ultimo e i dispositivi di storage riconosciuti dal proprio computer, siano essi dischi, dispositivi USB di storage, dischi di rete, NAS e sistemi di Cloud storage on-line.

Grazie a specifici driver a livello kernel, ogniqualvolta un'applicazione di qualsiasi tipo richiede di accedere a un file o disco criptato, se autorizzata, IndependenceKey entra in gioco decriptando e criptando in tempo reale i buffer dati (parti dei file) che l'applicazione stessa richiede durante il suo funzionamento. Le applicazioni credono di lavorare sempre e solo su file in chiaro, mentre in realtà operano su file criptati, ma senza la necessità di alcuna modifica o aggiornamento: **ogni applicazione presente nel computer, anche datata, può operare direttamente sui propri file in maniera sicura.** I file non vengono mai decriptati, da nessuna parte.

Se è selezionata l'opzione di cancellazione automatica dei file che vengono crittografati, IndependenceKey effettua la cancellazione totale (wiping) della versione in chiaro dei file che sono stati crittografati.



APRIRE – MODIFICARE

Per aprire un file criptato tramite IndependenceKey è necessario che la stessa sia inserita nel computer e sia stata sbloccata. **Il file non deve essere prima decriptato**, è sufficiente un semplice doppio click sul file per aprirlo. Si può agire sul file, fare modifiche come al solito senza cambiare le proprie abitudini di lavoro e continuando a utilizzare gli stessi strumenti di sempre. **Il file si apre automaticamente con l'applicazione ad esso correlata** (ad esempio, un file ".docx" si aprirà con Microsoft Word, Wordpad o con l'editor di testi installato nel proprio computer) **e si lavora direttamente sul file criptato**. Quando si chiude l'applicazione, registrando le modifiche apportate, IndependenceKey aggiorna automaticamente il file criptato.

Per nessun motivo verranno realizzate copie in chiaro del file sul proprio computer: l'applicazione di volta in volta utilizzata opera, tramite IndependenceKey, direttamente sul file criptato.

DECRIPARE

Per decriptare un file basta cliccare con il pulsante destro su uno o più file già criptati e scegliere l'opzione "IndependenceKey" -> "Decrypt". I file verranno decriptati automaticamente.

CRIPARE UNA DIRECTORY

Così come si possono crittografare uno o più file, è possibile criptare una intera directory. È sufficiente cliccare sulla directory con il pulsante destro del mouse, quindi selezionare "IndependenceKey" -> "Encrypt". Tutto il contenuto verrà automaticamente criptato. Se all'interno vi sono ulteriori directory con altri file, questi verranno a loro volta automaticamente criptati.

ATTENZIONE: Se si aggiunge un file in chiaro all'interno di una directory criptata il file non viene automaticamente criptato perché la funzione "Encrypt" crittografa i file nel momento in cui viene eseguita.

Per far sì che il contenuto di una directory sia sempre criptato, anche se si aggiungono file in un secondo momento, è opportuno utilizzare i dischi criptati di IndependenceKey (vedere il capitolo dedicato al servizio QDisk).

Più in dettaglio

IndependenceKey accede ai file e ai dischi crittografati seguendo le richieste delle applicazioni di alto livello. Per esempio, se si apre un file video crittografato riproducendolo con Windows Media Player o altro software multimediale e si esegue il "seek", ovvero la ricerca in avanti, saltando qua e là ne file A/V stesso, **IndependenceKey segue le richieste dell'applicazione accedendo dinamicamente al file criptato, allineandosi in tempo reale al punto di ingresso crittografico più vicino** e iniziando a decriptare quanto richiesto. L'algoritmo sviluppato da Quantec, basato sull'AES 256, consente di **adattare dinamicamente tali "punti di ingresso" in funzione del tipo di file**. Questo va a beneficio dei tempi di accesso in modalità casuale (random) ai file e dischi protetti e ottimizza la loro sincronizzazione durante l'aggiornamento su sistemi di Cloud storage e server aziendali, **trasferendo di volta in volta solo le modifiche strettamente necessarie** (diminuzione dei dati trasferiti, della banda e del tempo necessario).



QDisk

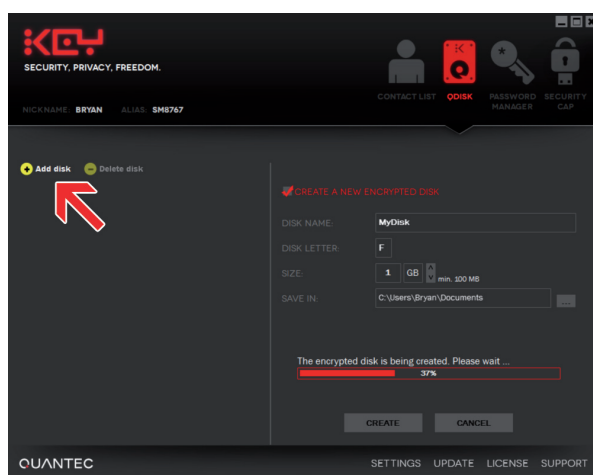
Creare un disco criptato

ASPETTI TECNICI

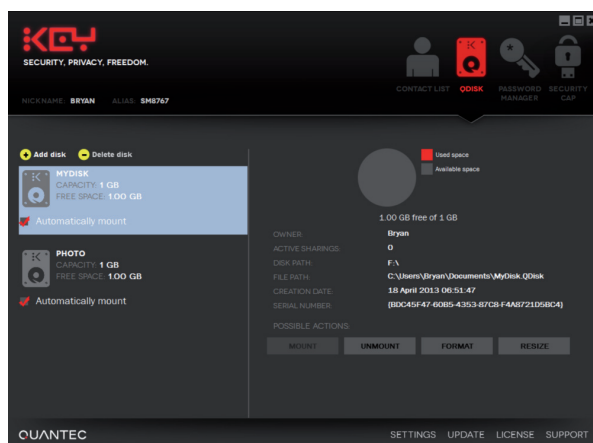


Per creare un disco criptato, aprire l'interfaccia utente e cliccare sull'icona QDisk.

Quindi selezionare "Aggiungi Disco" ("Add Disk") e compilare i campi che si aprono a destra dell'interfaccia come desiderato, scegliendo una lettera preferenziale per il disco con la quale, IndependenceKey, cercherà di montarlo nel sistema locale se disponibile (se non è disponibile, IndependenceKey utilizzerà la prima lettera libera utilizzabile).



Dopo aver cliccato sul pulsante "Create" al termine della procedura il disco verrà creato e comparirà in Windows come un normale disco, come quando si inserisce un qualsiasi dispositivo USB di storage in una porta USB del proprio computer.



A questo punto il disco è pronto all'uso. È possibile utilizzarlo come un qualsiasi disco: copiarci file, creare cartelle, spostare file, rinominarli, etc..

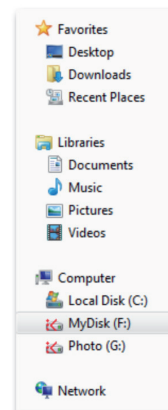
Se si vuole utilizzare un disco protetto già creato con IndependenceKey è necessario montarlo. Ciò può essere fatto tramite l'interfaccia di QDisk oppure, semplicemente, **facendo doppio click sul file immagine criptato che contiene il disco (tale file contiene tutta la struttura del disco ed è accessibile tramite Windows Explorer. Per ulteriori informazioni, vedere qui a destra)**. Il disco dispone anche dell'utile opzione "Automount" che consente, se abilitata, di montarlo automaticamente dopo aver inserito la propria Master Password, ovvero dopo aver sbloccato la propria IndependenceKey. È un'opzione molto utile per automatizzare le procedure di accesso ai propri dischi criptati.

Come funziona un disco protetto con IndependenceKey?

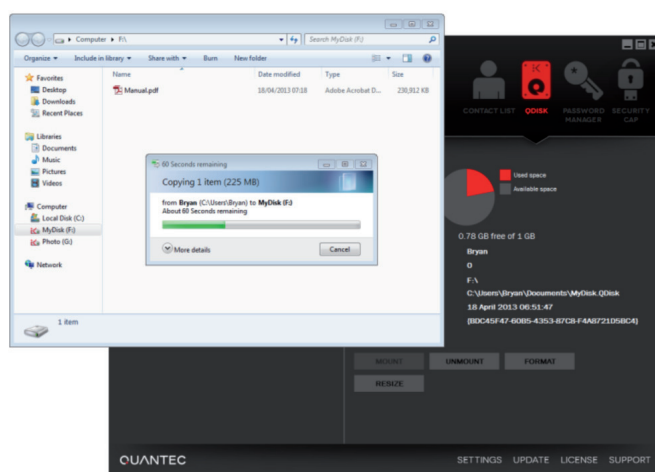
Un disco è organizzato per blocchi di archiviazione dei dati, denominati "cluster". Il file system del computer organizza e gestisce per conto del sistema operativo tali aree di storage, in maniera automatica e completamente astratta per l'utente e le applicazioni. All'interno del file immagine del disco denominato anche "file container", IndependenceKey crea e gestisce l'architettura fisica del disco, ovvero l'indicizzazione e gestione dei cluster. Esistono diversi tipi di cluster, alcuni raccolgono dati sulla struttura dei file, altri delle directory, altri contengono i dati veri e propri anche di più file e così via, come avviene in qualsiasi dispositivo di storage. **IndependenceKey agisce direttamente e in tempo reale sui cluster in forma esclusivamente criptata.** Come avviene nel caso dei file con le applicazioni installate sul proprio computer (vedi capitoli precedenti), in questo caso il **file system del sistema operativo accede direttamente ai cluster criptati, ma senza accorgersi di lavorare su cluster criptati!** IndependenceKey si pone nel mezzo e rende tutto questo processo completamente automatico e trasparente per il sistema operativo stesso.

Quanto può essere grande il disco?

Il disco non ha limiti di spazio. In fase di creazione o ridimensionamento è possibile definire la dimensione massima (ovviamente inferiore allo spazio libero disponibile sul disco fisico che lo ospita). Non è possibile ridurre le dimensioni di un disco che già contiene dei dati se si sceglie, come nuova capacità, un valore inferiore alla dimensione complessiva dei dati presenti. In questo caso occorre creare lo spazio necessario, cancellando alcuni file.



Il contenuto del disco è totalmente criptato via hardware tramite IndependenceKey e senza essa è impossibile accedervi. Come con qualsiasi dispositivo di storage, mentre si effettuano operazioni con il disco IndependenceKey non deve essere rimossa, altrimenti si possono corrompere i file sui quali si sta lavorando. L'engine QDisk di IndependenceKey rappresenta l'operatività del disco tramite le progress bar di avanzamento standard di Windows Explorer:



Per esempio, durante la copia di un file, quando la progress bar raggiunge il 100%, la finestra si chiude: significa che il disco ha terminato il suo lavoro e il file è stato completamente copiato e crittografato.

Se per qualsiasi motivo si esegue lo smontaggio (unmount) di un disco mentre si sta copiando al suo interno un file, IndependenceKey termina prima l'operazione in corso e poi smonta il disco automaticamente. In questo caso l'informazione appare tramite un fumetto (balloon hint) sulla system tray bar in basso a destra.

In futuro IndependenceKey supporterà anche dischi a dimensione variabile, in grado di adattarsi via via in funzione dei file e delle cartelle in essi inseriti. Per un uso su sistemi Cloud si consiglia l'uso dei dischi a dimensione fissa. In questo modo, IndependenceKey riesce ad ottimizzare la "cluster chain" ogni volta che si opera sui dischi stessi e i servizi di sincronizzazione di terzi (i.e. Dropbox, Google Drive, Power Folder, etc..) riescono a lavorare in maniera efficiente, sincronizzando solo le modifiche effettuate di volta in volta. Cosa che avviene anche con i dischi a dimensione variabile, ma con un grado di efficienza minore.

Si tenga presente che **quando si estrae IndependenceKey il sistema effettua lo smontaggio automatico di tutti i dischi al momento attivi**. L'effetto è che il disco scompare da Windows Explorer. Anche se tale operazione è possibile, si consiglia sempre di effettuare la rimozione sicura ("Safe Remove") della propria IndependenceKey (vedi il capitolo specifico) prima di estrarla oppure di eseguire l'unmount del disco. Se i dischi sono inattivi è comunque possibile estrarre IndependenceKey "a caldo", ovvero senza effettuarne la rimozione sicura. Invece, se il dispositivo viene forzatamente rimosso mentre si stanno copiando file oppure un programma esegue un salvataggio dati in un disco protetto, i file in fase di scrittura potrebbero risultare corrotti, così come avviene con qualsiasi dispositivo di storage rimovibile. Pertanto, **si consiglia di effettuare sempre la rimozione sicura della propria IndependenceKey oppure l'unmount dei dischi prima di rimuoverla**.

Cosa rimane del disco se tolgo IndependenceKey?

I dischi protetti, a prescindere dai contenuti in essi memorizzati, vengono organizzati e gestiti da IndependenceKey tramite dei "file container" ovvero dei "file immagine" che contengono tutta la struttura dei cluster costituenti i vari dischi. Tali file hanno estensione QDisk e contengono un'immagine totalmente criptata di ogni disco. Ogni disco corrisponde a un file container.

Una volta estratta IndependenceKey dal computer, sul dispositivo di storage dove sono presenti i file immagine QDisk (il disco principale del computer, un disco di rete, un NAS, un sistema di Cloud storage, etc..) **rimangono solo tali file completamente criptati**. Ad esempio, se si crea un disco "Mio Disco" da 10 GByte sul desktop del computer, esisterà in "C:\Users\Utente.Company\Desktop" un file da 10 GB denominato "Mio Disco.QDisk". Stesso discorso se il disco viene creato nella cartella di Dropbox o di qualsiasi altro posto dove si hanno i permessi di accesso.



Cloud storage sicuro con IndependenceKey



IndependenceKey può essere utilizzata per mettere al sicuro i tuoi dati nel Cloud.

I file possono essere criptati e copiati in qualunque spazio Cloud. Per accedere ai file criptati è sufficiente cliccarci sopra due volte come se non fossero criptati, al resto pensa IndependenceKey. Per poter aprire i file e i dischi protetti caricati sul Cloud è necessario che sia installato il software di IndependenceKey.

Grazie a IndependenceKey potrete accedere al vostro spazio Cloud, aprire i documenti e lavorare senza lasciare traccia. È sempre possibile ricorrere al camuffamento (scrambling) anche dei nomi dei file. In questo modo, non solo il contenuto del singolo file, ma anche il suo nome risulterà del tutto incomprensibile. Solo inserendo IndependenceKey sarà possibile visualizzare il nome reale del file.

SINCRONIZZARE FILE E DISCHI IN DROPBOX

I sistemi di Cloud storage come Dropbox, Power Folder e altri, eseguono sui propri server una copia differenziale dei file che l'utente carica nel proprio spazio on-line. IndependenceKey **protegge il contenuto di questi file** grazie a un avanzato e intelligente utilizzo della crittografia, **consentendo al tempo stesso di continuare a lavorare sui file senza cambiare le proprie abitudini**.

Prima di tutto occorre disporre di un proprio spazio sul Cloud. Dropbox, per esempio, offre fino a 2 GByte gratuiti. Seguire le procedure indicate dal software del fornitore per creare il proprio spazio sul Cloud. Una volta creato, lo spazio sul Cloud è generalmente accessibile attraverso Windows Explorer sotto forma di cartella, link preferito o disco. Per utilizzare il Cloud in maniera sicura è sufficiente mettere i file criptati all'interno di tale spazio oppure criptare i file in chiaro già esistenti cliccandoci sopra con il pulsante destro e scegliendo l'opzione "IndependenceKey" -> "Encrypt".

Lo stesso vale per i dischi protetti con IndependenceKey. È sufficiente creare i propri dischi criptati QDisk all'interno del proprio spazio Cloud oppure trasferirvi quelli già esistenti, facendo sempre attenzione allo spazio disponibile in funzione del proprio contratto. Si ricorda che per spostare un disco QDisk questo deve essere smontato (opzione "unmount" nell'interfaccia utente, sezione QDisk), ovvero non deve risultare in uso. Lo spostamento può essere effettuato come di consueto tramite CTRL+X e CTRL+V oppure Drag & Drop scegliendo l'opzione "Sposta qui" ("Move here").

Una volta creato o spostato il disco nell'area di Cloud storage è sufficiente un doppio click sul file QDisk stesso per montarlo. È possibile anche utilizzare l'opzione "Automount" in modo che il disco venga automaticamente aperto e montato ogni volta che si inserisce la propria IndependenceKey nel computer e la si sblocca tramite la Master Password. L'opzione "Automount" è disponibile tramite l'interfaccia utente, nella sezione QDisk, nelle proprietà del disco.

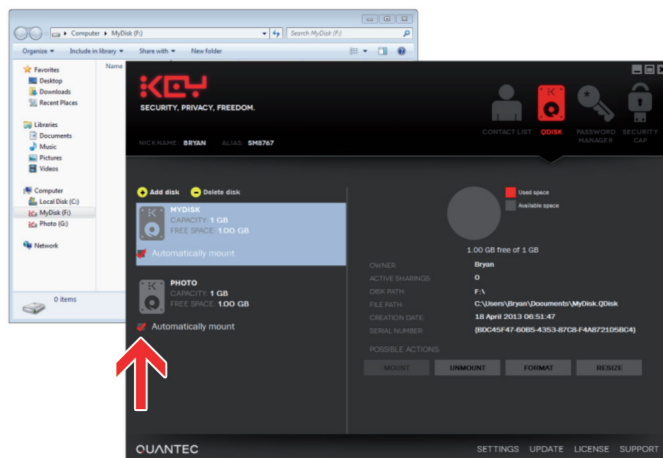
ASPETTI TECNICI

Cos'è il Cloud Storage?

È una modalità di archiviazione e accesso ai propri dati prettamente on-line, che richiede la presenza della connettività Internet. L'utente può memorizzare i propri dati nel proprio spazio di Cloud storage per potervi poi accedere in ogni momento, in alcuni casi anche tramite web browser, anche da più computer e dispositivi e disporre di una copia di backup sempre aggiornata. Alcuni servizi di Cloud storage offrono anche il versionamento dei file, ovvero memorizzano in maniera incrementale le varie modifiche, consentendo all'utente di recuperare le versioni precedenti dei propri file e documenti nei limiti dello spazio di storage da quest'ultimo acquistato. Il più famoso e funzionale tra questi servizi è Dropbox, ma ne esistono altri come Power Folder, etc..

Come funziona?

Prendendo in esame Dropbox, viene creata sul computer dell'utente un'area gestita e monitorata dal servizio di Cloud storage: ogni volta che si posiziona un file in tale area, o si crea una directory, oppure si rinomina un file e così via, il sistema sottostante sincronizza sul server del fornitore le differenze rendendo disponibile il file aggiornato anche sugli altri computer sincronizzati con l'account dell'utente. La sincronizzazione avviene generalmente quando il singolo file modificato viene rilasciato dall'applicazione.



I servizi di Cloud storage come Dropbox eseguono una copia differenziale dei file presenti nell'area di Cloud storage sui propri server. Quando si aggiorna un file criptato oppure si lavora su un disco protetto, si apportano delle modifiche alla struttura dati. Queste modifiche vengono automaticamente trasferite dal servizio di Cloud storage non appena il file viene rilasciato dall'applicazione con cui è stato gestito (ad esempio, si chiude Microsoft Word dopo aver salvato il proprio lavoro su di un documento). Affinché ciò avvenga anche con i dischi, è necessario che questi vengano smontati.

Tornando all'esempio, se si crea e gestisce dentro Dropbox un disco protetto da 2 GByte e, durante il suo utilizzo, si copiano in tale disco 10 MByte di dati, una volta smontato il disco Dropbox lo sincronizzerà inviando sui propri server poco più di 10 MByte di dati, totalmente criptati. Inserendo la propria IndependenceKey in un altro computer sincronizzato con il medesimo account Dropbox e montando il disco, questo apparirà nelle risorse del computer locale con i dati aggiunti esattamente come li si era lasciati. **File e dischi sono totalmente criptati e protetti dalla propria IndependenceKey.** È finalmente possibile utilizzare il Cloud in assoluta sicurezza e tranquillità.

Qual è il ruolo di IndependenceKey?

IndependenceKey rende del tutto inaccessibile il contenuto dei file e dei dischi posizionati nei server dei fornitori dei servizi di Cloud storage e, soprattutto, grazie al proprio engine crittografico adattivo a blocchi variabili, consente di mantenere l'assoluta riservatezza in AES 256 e, nel contempo, di **aggiornare tali file e dischi in maniera incrementale**. Quando un file viene crittografato, data una chiave di crittografia "X", questo assume una morfologia completamente diversa dall'originale, ovvero viene trasformato in una sequenza di bit ad altissima entropia (caotica), sostanzialmente senza senso alcuno. Il processo crittografico che porta a generare tale sequenza è, per sua natura, di tipo "chained" ovvero opera a blocchi sequenziali. Il blocco alla posizione n-1 influenza la crittografia del blocco alla posizione n successiva. Per questo motivo, se si cambia il contenuto del primo blocco, a parità di chiave crittografica ("X" nell'esempio), tutta la sequenza di bit risultante (bitstream) è completamente diversa dalla precedente. Si pensi ora a un file di grandi dimensioni, a un data base o, meglio, all'immagine (file container) di un disco QDisk protetto: se si operasse esclusivamente in modalità "chained", aggiungendo anche solo un piccolo documento nel disco, il processo crittografico modificherebbe l'intera sequenza di bit dal cluster nel quale ha avuto l'inserimento in poi, rendendo la sincronizzazione sul Cloud del disco stesso di fatto impossibile. Ad esempio, se il disco fosse di 1 GByte e si aggiungessero anche solo 100 kByte di dati all'inizio, tutta la sequenza di bit costituenti il disco cambierebbe. Proprio in questo IndependenceKey fa la differenza: **l'engine crittografico di IndependenceKey va a modificare solo i blocchi interessati e quelli immediatamente adiacenti**, mantenendo l'integrità crittografica dell'intero file. Quando il file viene rilasciato dall'applicazione (si chiude Word, ad esempio, nel caso del singolo file o si smonta il disco nel caso dei QDisk), il servizio di sincronizzazione differenziale sottostante del fornitore dello spazio Cloud rileva solo piccole differenze e, quindi, esegue la sincronizzazione rapidamente.

Da questo trae beneficio anche la sincronizzazione dei file protetti con IndependenceKey posizionati nel Cloud quando si modificano i diritti di accesso (share) ai file stessi. Se un utente vuole consentire a un altro di aprire un file già crittografato e presente sullo spazio Cloud condiviso (come su di un server aziendale, NAS e così via) è questione di pochi secondi e l'autorizzazione viene automaticamente estesa a tutti i sottoscrittori del servizio.



Associazione con altri utenti

ASPETTI TECNICI



IndependenceKey può essere associata con altre IndependenceKey. Associare due IndependenceKey significa abilitare due utenti a scambiarsi file in maniera sicura e ad accedervi e modificarli in tutta tranquillità. In futuro saranno resi disponibili ulteriori servizi aggiuntivi, opzionali, come la possibilità di effettuare telefonate VoIP sicure e scambiarsi messaggi sicuri.

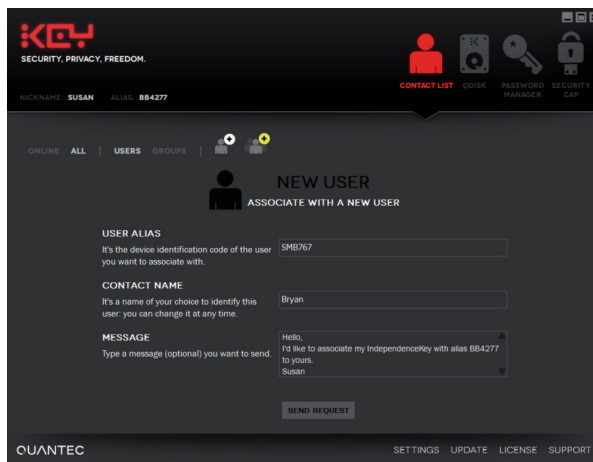
Associarsi con un utente non significa abilitarlo ad accedere a ogni file, dato e disco protetto. Significa vederlo apparire nella propria "Lista Contatti" ("Contact List") e potere scegliere, di volta in volta, se condividere o meno un dato file. **Le autorizzazioni di accesso a un file conferite a un utente possono essere rimosse dal medesimo file solo da chi lo ha creato,** ovvero da chi lo ha inizialmente crittografato.

L'operazione di associazione può essere svolta in due modi:

ASSOCIAZIONE REMOTA

Gli utenti non hanno modo di incontrarsi

Aprire l'interfaccia -> Selezionare dal menù "Users" -> "Contact List" e per aggiungere un utente cliccare sull'icona evidenziata in figura:



The screenshot shows the IndependenceKey web interface. At the top, there's a header with the 'KEY' logo and the tagline 'SECURITY, PRIVACY, FREEDOM.' Below this, a navigation bar includes 'CONTACT LIST', 'DISK', 'PASSWORD MANAGER', and 'SECURITY CAP'. The main content area is titled 'NEW USER' and 'ASSOCIATE WITH A NEW USER'. It contains a form with the following fields: 'USER ALIAS' (with a value of 'SM8767'), 'CONTACT NAME' (with a value of 'Bryan'), and 'MESSAGE' (with a pre-filled text: 'Hello, I'd like to associate my IndependenceKey with alias BB4277 to yours. Susan'). A 'SEND REQUEST' button is at the bottom of the form. The footer of the interface includes the 'QUANTEC' logo and links for 'SETTINGS', 'UPDATE', 'LICENSE', and 'SUPPORT'.

Nella schermata che si apre digitare l'Alias della persona che si sta cercando (nell'esempio, l'utente Susan sta inviando una richiesta di associazione all'utente Bryan che, in precedenza, ha comunicato il suo Alias a Susan).

L'Alias è un codice univoco derivato anche dal serial number del chip di autenticazione crittografica di IndependenceKey e dai segreti combinatori di fabbrica. Ogni utente dispone del proprio esclusivo Alias che può comunicare agli altri utenti per attivare l'associazione remota. L'Alias, insieme al Nickname, è sempre ben evidente nell'interfaccia utente, posizionato in alto a sinistra sotto il logo di IndependenceKey.

Come funziona l'associazione?

L'associazione tra due utenti, ovvero tra due IndependenceKey, è un procedimento matematico basato su algoritmi crittografici e di autenticazione. Al suo interno, IndependenceKey dispone sia di un motore crittografico che di un chip crittografico di autenticazione dedicato, appartenente alla piattaforma TPM (Trusted Platform Module).

Grazie a questo chip e al suo motore crittografico, quando due IndependenceKey si associano effettuano, prima di tutto, una verifica di genuinità. Solo dopo questa verifica si scambiano dei segreti univoci e irripetibili che permettono alle due IndependenceKey di riconoscersi, stabilire canali di comunicazione sicuri e scambiarsi file e informazioni in maniera riservata e totalmente protetta.

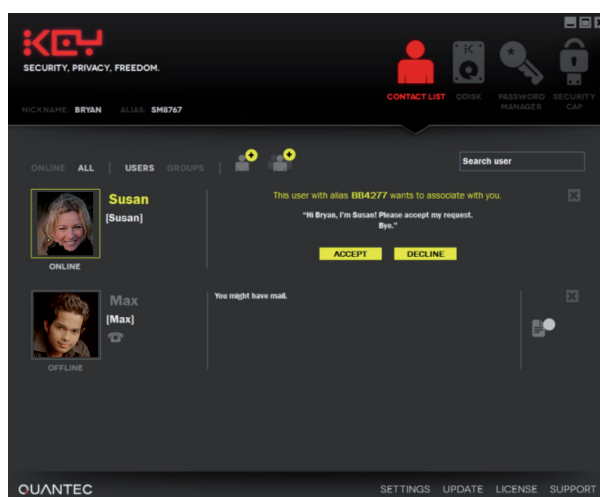
L'associazione remota è meno sicura di quella fisica locale?

No. IndependenceKey può associarsi ad altre IndependenceKey sia fisicamente, collegando l'una all'altra grazie alla porta USB posteriore, sia remotamente tramite Internet. In entrambi i casi i chip crittografici di autenticazione interni consentono ai due dispositivi di dialogare in maniera implicitamente sicura a livello hardware, di effettuare le verifiche necessarie, criptare il canale di comunicazione, nonché generare e scambiarsi in maniera sicura i segreti combinatori univoci necessari per completare l'associazione.

L'Alias può essere comunicato all'altra persona con cui ci si vuole associare anche in modo pubblico. Non è un dato sensibile e anche se letto da terzi non può essere utilizzato per falsificare l'identità.

Una volta digitato l'Alias della IndependenceKey remota con cui ci si vuole associare è possibile inserire il Nickname con il quale, successivamente, si vuole riconoscere l'altra persona nella propria lista contatti ("contact list") e digitare un breve messaggio di testo accompagnatorio. Infine cliccare -> "Invia" ("Send") per inviare la richiesta.

Non appena l'altra persona sarà on-line con la propria IndependenceKey, riceverà la richiesta di associazione, visualizzandola tramite la propria interfaccia utente:



Appena il destinatario accetta la richiesta, il mittente (Susan, nell'esempio) compare nella sua Contact List. Analogamente il destinatario appare nella Contact List del mittente.

Non è necessario che entrambi siano on-line nello stesso istante. L'operazione può avvenire in maniera differita, tramite i server Quantec. Per i dettagli, vedere le note tecniche a lato.

È possibile associarsi con un numero molto elevato di utenti (diverse migliaia) ed è sempre possibile eliminare le associazioni non più desiderate. Eliminandole, non sarà più possibile accedere ai file che erano stati condivisi da tali utenti (ovviamente, è sempre possibile accedere ai file condivisi a tali utenti, anche se eliminati dalla propria Contact List).

Cosa fanno i server di Quantec durante l'associazione remota?

Quantec rende disponibile un servizio di relay (rilancio) dei pacchetti di comunicazione tra due IndependenceKey che consente di sostituire Internet al mezzo di comunicazione USB utilizzato durante l'associazione fisica locale. **I pacchetti escono fisicamente già criptati a priori da ogni IndependenceKey**, raggiungono i server che li memorizzano finché l'IndependenceKey con la quale ci si vuole associare si collega ad Internet. **I server di Quantec non sono in grado di conoscere i segreti che le due IndependenceKey si scambiano**, ma si limitano a identificare entrambi i dispositivi tramite il loro identificativo univoco universale ovvero l'Alias. Lo scopo dei server è quello di consentire a due utenti di potersi associare utilizzando Internet in qualsiasi momento, senza la necessità che entrambi siano on-line nel medesimo istante e senza instaurare un canale di comunicazione diretto attraverso la porta USB posteriore.

Associarsi significa dare l'accesso incondizionato a tutti i file protetti?

Assolutamente no! Associarsi con un altro utente significa generare i segreti combinatori necessari per poter stabilire, in quel momento o successivamente, una sessione di comunicazione sicura e in tempo reale, oppure condividere in maniera sicura i file ai quali si è fornita l'autorizzazione di accesso tramite la funzione "Crypt & Share" di IndependenceKey.



Associazione con altri utenti

ASSOCIAZIONE FISICA

Gli utenti hanno modo di incontrarsi

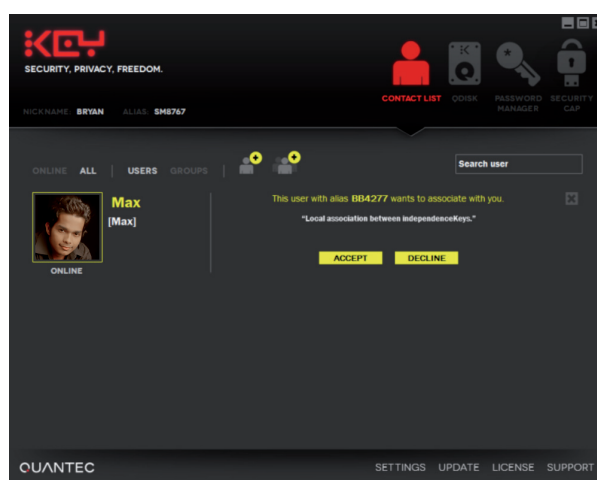
IndependenceKey può associarsi a un'altra IndependenceKey fisicamente inserendo l'una nella porta USB posteriore dell'altra!



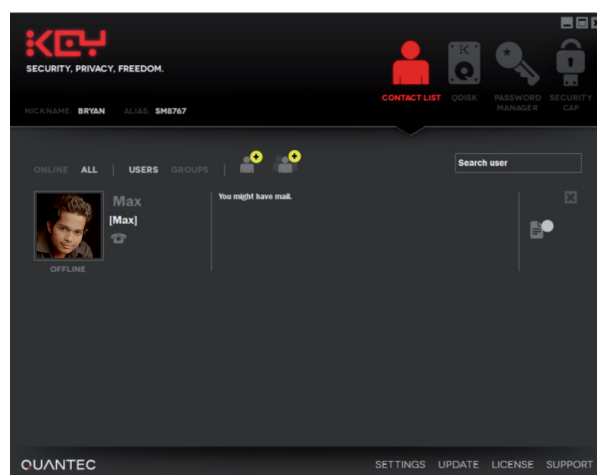
Per realizzare un'associazione fisica inserire la propria IndependenceKey nel computer e sbloccarla. Inserire quindi l'IndependenceKey della persona con la quale ci si vuole associare nella propria IndependenceKey. Dopo alcuni istanti comparirà sul proprio computer una finestra con la richiesta di inserire la Master Password dell'IndependenceKey con la quale ci si vuole associare, ciò perché deve esserci sempre il consenso del relativo proprietario.

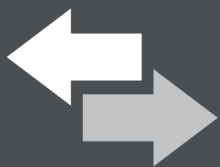
Se la Master Password è corretta e le due IndependenceKey non sono già associate viene chiesto se si vuole procedere e, se si risponde di sì, si conclude la procedura.

Nell'esempio, Bryan accetta la richiesta di connessione locale, fisica, di Max che ha inserito la sua IndependenceKey in quella di Bryan. La Master Password che è stata richiesta dal sistema è quella della IndependenceKey di Max



A questo punto i due utenti appaiono l'uno nella Contact List dell'altro e possono iniziare a condividere file e comunicare in maniera sicura e protetta.





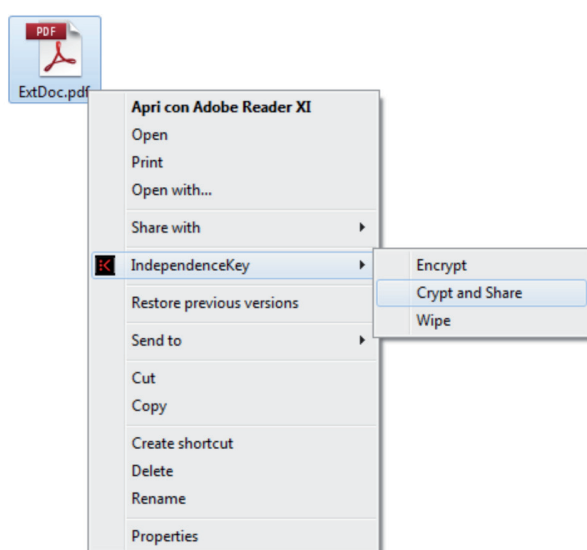
Condivisione protetta delle informazioni

ASPETTI TECNICI

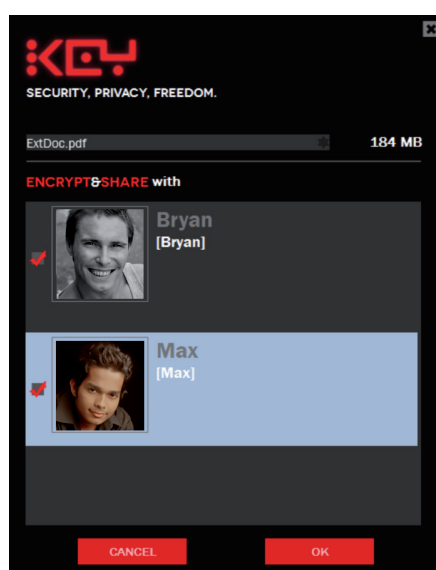
 Dal momento in cui ci si associa con altri utenti è possibile iniziare a condividere informazioni, in particolare file o gruppi di file.

PER CONDIVIDERE UN FILE

Per condividere un file, fare click con il pulsante destro sul file per aprire il menù contestuale di Windows, selezionare -> "IndependenceKey" -> "Crypt & Share"



Si apre un pannello indicante tutti i contatti presenti nella propria rubrica. Selezionare i contatti che si desidera abbiano accesso al file cliccandoci sopra.



Come fa IndependenceKey a gestire i diritti di accesso a un file?

I file criptati con IndependenceKey dispongono di una propria struttura dati, completamente crittografata e appositamente progettata per consentire al sistema operativo di interagire con tali file come con qualsiasi altro file presente nel computer.

Ogni file protetto con IndependenceKey viene criptato mediante l'algoritmo a blocchi adattivo di Quantec utilizzando l'AES 256 e contiene, al suo interno, diversi riferimenti ai dati salienti del file come il nome reale del file (ricordiamo che con IndependenceKey è possibile addirittura eseguire lo scrambling (camuffamento) dei nomi dei file e non solo crittografarli), la tipologia del file, la sua dimensione e così via.

Tra questi elementi vi è la sequenza di utenti che può accedere al singolo file. Gli utenti che sono autorizzati ad accedere al file vengono identificati tramite un codice univoco e universale generato durante la fase di associazione.

Quando un utente tenta di aprire un file crittografato con IndependenceKey, il driver di sistema installato su Windows attraverso il software in dotazione con IndependenceKey accede a una piccola parte del file, la decripta all'interno della IndependenceKey e verifica se l'utente conosce la chiave con cui il file è stato crittografato. Se tale chiave è nota allora il file viene processato, ovvero aperto, decriptato e inviato all'applicazione a cui fa riferimento, altrimenti no. La chiave crittografica viene ricostruita a partire dai segreti combinatori dell'algoritmo di associazione tra utenti diversi, che sono protetti nei chip crittografici di IndependenceKey.

Il procedimento con cui viene realizzato tutto ciò è totalmente hardware e si basa sempre sul principio che le chiavi non lasciano mai IndependenceKey. Per questo motivo, ogni operazione crittografica, di autenticazione e verifica dell'integrità del file stesso avviene all'interno di IndependenceKey.

Questa soluzione consente non solo di decriptare un file, ma anche di verificarne l'integrità strutturale.

IndependenceKey crittografa automaticamente il file, se non era già crittografato, e ne estende i diritti di accesso agli utenti selezionati. Non è necessario crittografare prima il file e poi estenderne i diritti. **In qualsiasi momento è possibile estendere o rimuovere i diritti di accesso a un file già crittografato.** Il file così criptato può essere inviato in totale sicurezza utilizzando le modalità già in uso, anche le più insicure, come la posta elettronica, Skype, siti di file transfer e così via.

Grazie a IndependenceKey non è necessario condividere alcun segreto, password, chiave di crittografia o altro. Niente più password di accesso inviate via email, SMS o lette al telefono. L'Utente che riceve il file e che è abilitato ad accedervi, se ha la propria IndependenceKey inserita e sbloccata nel proprio computer, non deve decriptare il file. È sufficiente che faccia un doppio click sul file per aprirlo e modificarlo a piacimento. **Non è necessario cambiare abitudini di lavoro:** alla fine basta salvare come sempre il lavoro fatto e IndependenceKey aggiorna automaticamente il file criptato.

Con IndependenceKey si lavora sempre direttamente sul file criptato.

PER CONDIVIDERE PIU' FILE

È possibile condividere molti file e cartelle in maniera sicura. Se si selezionano, ad esempio, 5 file non criptati e si esegue l'opzione "Crypt & Share", tali file verranno criptati automaticamente in un'unica operazione. La finestra di avanzamento di IndependenceKey riporta, in tempo reale, lo stato di avanzamento di ogni operazione in corso.

Se tra i file selezionati ve ne è uno già criptato, come di consueto verrà richiesto di scegliere con chi condividere i 4 file da criptare, ma apparirà anche un'ulteriore richiesta specifica per il file già criptato. Infatti, prima di modificare i diritti di accesso a file già criptati, occorre verificare con chi sono già condivisi. Quest'ultima operazione può essere svolta solo dall'utente che ha creato tali file criptati.

AGGIUNTA/RIMOZIONE DEI DIRITTI

Un file già criptato e condiviso con alcuni utenti può essere condiviso con altri nuovi utenti estendendone i diritti. È sufficiente ripetere la procedura sopra indicata, ovvero click destro sul file -> "IndependenceKey" -> "Crypt & Share", senza dover decriptare prima il file.

In maniera analoga, è possibile rimuovere gli utenti dai diritti di accesso al file, sempre seguendo la medesima procedura.

UTENTE OWNER O PROPRIETARIO DEI DIRITTI

Solo l'utente che ha creato il file può modificarne i diritti di accesso, vale a dire che se l'utente A crea un file criptato e ne estende i diritti di accesso anche agli utenti B e C, questi non potranno a loro volta estenderne i diritti ad altri utenti oppure rimuovere uno degli altri utenti: dovranno sempre interagire con l'utente A (owner o proprietario del file) per poter modificare i criteri di condivisione.

In futuro IndependenceKey consentirà anche di conferire i diritti di sola lettura a un dato file, la possibilità di consentire un numero massimo di aperture del file o di fissare una data di scadenza al file stesso, superata la quale nessun utente potrà aprirlo tranne il proprietario (l'utente A nell'esempio precedente).

SINCRONIZZAZIONE DEI FILE CRIPTATI E DIRITTI

Seguendo la procedura sopra indicata il proprietario del file può modificarne i diritti in ogni momento. Bisogna però tenere presente che, se il file non risiede su un sistema di Cloud storage sincronizzato (i.e. Dropbox o simili) oppure su un server aziendale gli altri utenti potranno sempre continuare ad aprire le versioni precedenti dei file criptati già in loro possesso.

Dal punto di vista della sincronizzazione dei file, l'uso del Cloud rende più interattiva ed efficace la gestione degli accessi alle risorse protette, soprattutto quando a tali dati e informazioni devono accedere molti utenti con diritti diversi.

Utilizzo della porta USB host

ASPETTI TECNICI

 IndependenceKey è dotata di una porta USB host posteriore che può essere utilizzata per vari scopi:

- Collegare un'altra IndependenceKey
- Collegare il Security Cap
- Collegare il Data Bank
- Collegare una cuffia VoIP digitale
- Collegare una memoria USB di storage
- E, in futuro, collegare una tastiera USB o una microcamera USB

La presenza di questa peculiare funzionalità consente a IndependenceKey di erogare diversi utili servizi crittografici.

L'inserimento e la rimozione di tali dispositivi in/da IndependenceKey può avvenire "a caldo", ovvero con IndependenceKey già inserita e sbloccata nel proprio computer.

ESEGUIRE UN BACKUP CRIPTATO SU SUPPORTI ESTERNI

Tramite IndependenceKey è possibile crittografare file e dati su normali dispositivi USB di mass-storage, implicitamente insicuri, siano essi comuni "chiavette" USB oppure hard disk USB senza cambiare le proprie abitudini. Per far ciò è sufficiente **inserire tali dispositivi nella porta USB posteriore della propria IndependenceKey** precedentemente inserita nel computer e sbloccata.



Cos'è una porta USB Host?

Lo standard USB prevede diverse tipologie di interfacce e connettori, tutti riconducibili al mondo dei dispositivi USB, ma tra loro profondamente diverse. Una porta USB "host" è quella di un comune computer, ovvero quella dove si inseriscono dispositivi USB di tipo "device" come memorie USB di storage, hard disk USB, cuffie USB e così via.

IndependenceKey è dotata sia di una porta USB device, per potersi chiaramente collegare al computer, sia di una porta USB host alla quale collegare ulteriori dispositivi USB.

Grazie ad alcune soluzioni specifiche messe a punto da Quantec, l'integrazione elettronica raggiunta nel dispositivo ha consentito di ridurre le dimensioni di IndependenceKey ai minimi termini, mantenendo nel contempo le prestazioni di una porta USB 2.0 High-Speed, ovvero in grado di raggiungere i 480 Mbps di canale. Tramite la porta USB di tipo device, IndependenceKey viene vista dal computer come una scheda di rete ad alta velocità, grazie all'ingegnerizzazione hardware e ai driver installati nel computer con il software in dotazione.

Che limiti ha la porta USB host posteriore?

Lo standard USB impone che una porta USB host eroghi una certa corrente per poter alimentare correttamente il dispositivo ad essa collegato. Tale corrente deve essere almeno di 500 mA a 5 Volt. Diversi computer, oggi come oggi, erogano su alcune porte più corrente di quella minima richiesta dallo standard, ma non su tutte le porte. Ad esempio, alcuni hard disk USB, soprattutto se di vecchia generazione, richiedono di essere a loro volta alimentati esternamente e ricorrono a doppi connettori USB (per aumentare, la corrente a disposizione) oppure ad alimentatori esterni.

IndependenceKey è un dispositivo USB di tipo low-power (a basso consumo) ed è **in grado di adattare dinamicamente il consumo di energia in funzione delle attività svolte**. Tale caratteristica consente non solo di alimentare addirittura due IndependenceKey inserite l'una nell'altra durante la procedura di associazione fisica, ma anche di alimentare la maggior parte dei dispositivi USB di mass-storage, cuffie USB e così via. Tuttavia, se una volta inserito il proprio dispositivo in IndependenceKey questo non dovesse accendersi, occorre provare sulle altre porte USB del computer disponibili oppure collegare al dispositivo USB esterno il suo alimentatore supplementare.

Se IndependenceKey è già sbloccata, non appena vi si inserisce il dispositivo USB di storage, esso appare nell'interfaccia di Windows come avviene di consueto: il sistema operativo non si accorge della presenza di IndependenceKey.

A questo punto è sufficiente fare un Drag&Drop o un CTRL+C & CTRL+V dei file desiderati nel supporto esterno, ed essi verranno copiati e criptati automaticamente. Al termine della copia il supporto contiene i dati completamente protetti.

Per accedere successivamente a tali file non è strettamente necessario inserire il dispositivo USB di mass-storage nella porta USB host di IndependenceKey. Si può continuare a utilizzare anche la modalità tradizionale, inserendo il dispositivo USB in un'altra porta USB libera del computer.

L'accesso ai dati avviene come di consueto: basta disporre della propria IndependenceKey già inserita e sbloccata ed effettuare un doppio click per aprire il file.

Infine, i file contenuti su tali supporti esterni possono essere condivisi con terzi tramite l'opzione "Crypt & Share" di IndependenceKey, seguendo le indicazioni riportate nel paragrafo precedente. In questo modo è possibile inserire un comune dispositivo USB di storage nella propria IndependenceKey già sbloccata, copiarvi un file e condividerlo al collega con il quale ci si era associati in precedenza. Estrarre il dispositivo di storage e consegnarlo al collega. Quest'ultimo, a sua volta, con la propria IndependenceKey potrà accedere al file in maniera assolutamente sicura in ogni momento inserendo il dispositivo di storage nella porta USB posteriore della sua IndependenceKey oppure in una delle porte USB libere del computer nel quale è attiva la sua IndependenceKey.

Come prassi, prima di rimuovere il dispositivo USB di mass-storage da IndependenceKey occorre smontarlo così come si dovrebbe fare anche quando lo si rimuove da una porta USB generica del proprio computer. Se, tuttavia, viene rimosso forzatamente, IndependenceKey tenta a sua volta di chiudere la sessione di lavoro su tale dispositivo anche per il sistema operativo (Windows). Tuttavia, è bene assicurarsi che non ci siano file aperti sul dispositivo o copie in corso, altrimenti i file verranno persi o risulteranno inevitabilmente corrotti.

C'entra qualcosa il "Safe Unmount" con il dispositivo USB posteriore?

L'opzione "Safe Unmount" disponibile cliccando con il pulsante destro sull'icona di IndependenceKey nella System Tray Bar in basso a destra, riguarda la funzionalità di chiusura della sessione di lavoro di IndependenceKey. Consultare il capitolo "Estrazione di IndependenceKey" per ulteriori dettagli.



Utilizzo del Security Cap

BACKUP DELLE CHIAVI CRITTOGRAFICHE, ASSOCIAZIONI E PASSWORD MANAGER.

Durante l'uso IndependenceKey genera una serie di chiavi crittografiche uniche e irripetibili con le quali vengono gestiti i vari servizi di crittografia disponibili. Genera inoltre specifici segreti combinatori, a partire dalla fase di inizializzazione con l'inserimento della propria Master Password, e durante le fasi di associazione con altri utenti. Le chiavi crittografiche e i segreti combinatori non lasciano IndependenceKey in alcun modo.

Il Security Cap è la soluzione hardware, 100% crittografata e protetta, attraverso la quale l'utente può agevolmente eseguire i backup dei dati crittografici contenuti all'interno della propria IndependenceKey come e quando desidera, in totale autonomia e sicurezza rispetto a chiunque, ivi inclusa la stessa Quantec che ha progettato IndependenceKey!

Il Security Cap non esegue il backup dei file, dischi e cartelle crittografati con IndependenceKey, bensì archivia le chiavi crittografiche e tutti i dati necessari per poter accedere, ovvero decriptare, tali file. Il backup dei file criptati è a cura dell'utente.

Il Security Cap viene associato univocamente con IndependenceKey durante la fase di inizializzazione (per i dettagli riferirsi al capitolo specifico all'inizio di questo manuale).

Il Security Cap può essere sbloccato solo dall'utente proprietario mediante la medesima Master Password utilizzata con la propria IndependenceKey.

Per eseguire un backup è sufficiente inserire il Security Cap nella propria IndependenceKey sia già inserita nel computer e sbloccata che ancora da inserire nel computer e sbloccare.



ASPETTI TECNICI

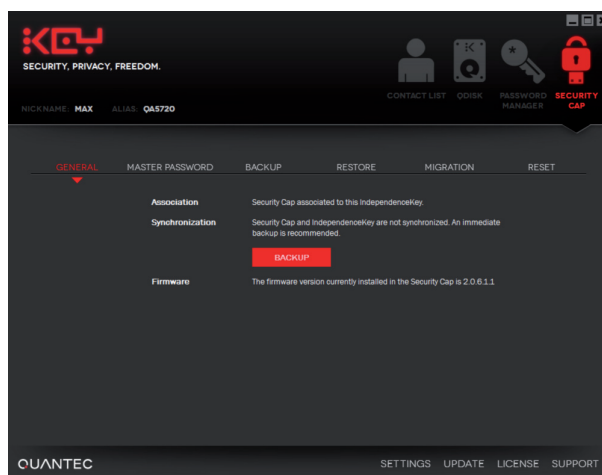
Il Security Cap è associato solo alla mia IndependenceKey o anche ad altre?

All'interno di IndependenceKey e all'interno del suo Security Cap è presente un chip crittografico di autenticazione della piattaforma di sicurezza TPM (Trusted Platform Module). Tramite tali chip, insieme ai rispettivi engine crittografici, IndependenceKey e il Security Cap si associano indissolubilmente tra loro durante la fase di associazione, effettuando tutte le verifiche di anticloning necessarie, criptando il canale di comunicazione e memorizzando, ognuno dei due dispositivi, parte dei segreti combinatori derivati dalla Master Password. In questo modo, il Security Cap è associabile solo alla propria IndependenceKey oppure a una nuova IndependenceKey in caso di furto o smarrimento. Attenzione: se non si dispone della Master Password, il Security Cap non può associarsi in alcun modo ad altre nuove IndependenceKey.

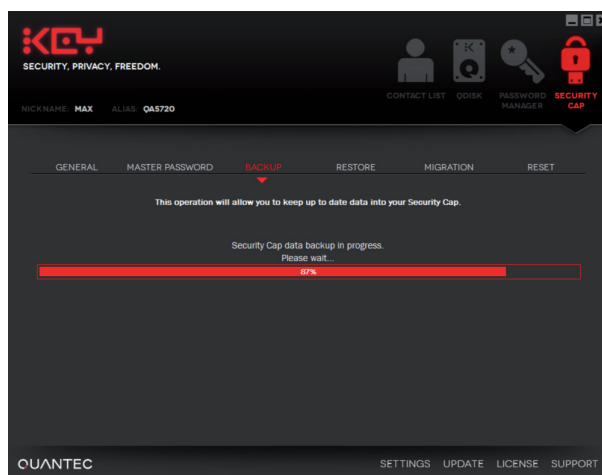
Perché se critto un file e poi inserisco il Security Cap non fa il back up?

Per ottimizzare l'uso dell'engine crittografico e, pertanto, anche la necessità di eventuali frequenti backup, IndependenceKey gestisce la crittografia dei file in maniera indicizzata, ovvero il file contiene solo un riferimento alla chiave crittografica da utilizzare, riferimento che è in grado di comprendere solo la propria IndependenceKey. Uno specifico algoritmo interno a IndependenceKey consente di utilizzare in maniera intelligente tali riferimenti correlando la crittografia del singolo file o disco non solo a una chiave crittografica, ma anche ad altri segreti combinatori presenti all'interno di IndependenceKey. Tale procedimento contempla la creazione di questi segreti solo nella fase di inizializzazione e ogniquale volta ci si associa con nuovi utenti. In questi casi è sempre consigliabile eseguire il backup della propria IndependenceKey.

L'interfaccia utente del software in dotazione si posiziona sulla schermata del Security Cap indicando, se necessario, la possibilità di eseguire il backup. Per eseguire il backup premere sull'apposito pulsante nell'interfaccia.



Il backup viene proposto automaticamente dall'interfaccia utente se IndependenceKey rileva una differenza nella versione del data base interno del Security Cap, ovvero rileva che IndependenceKey contiene dei dati più aggiornati di quelli presenti nel Security Cap. La procedura è tale per cui non è possibile inserire un Security Cap contenente un backup con una versione più recente di quella presente nella IndependenceKey con cui è associato.



Il backup prevede anche l'archiviazione sicura e automatica di tutti i dati presenti nel Password Manager.

Il Security Cap è una memoria di mass-storage?

Assolutamente no! Il Security Cap è un dispositivo USB crittografico a tutti gli effetti, dotato di un proprio microcontrollore crittografico ad alte prestazioni nonché dei chip di autenticazione della piattaforma TPM protetti a livello fisico dall'accesso esterno. A tutti gli effetti è un dispositivo della stessa classe e categoria di IndependenceKey e non si limita ad archiviare dati su una memoria flash interna come un normale dispositivo di mass-storage USB, bensì esegue una precisissima verifica di genuinità dell'IndependenceKey alla quale viene collegato, è in grado di criptare in AES 256 a sua volta il canale USB locale stabilendo una connessione sicura con la propria IndependenceKey e, infine, memorizza il backup integrale delle chiavi crittografiche in maniera totalmente criptata.

Che succede se perdo il Security Cap?

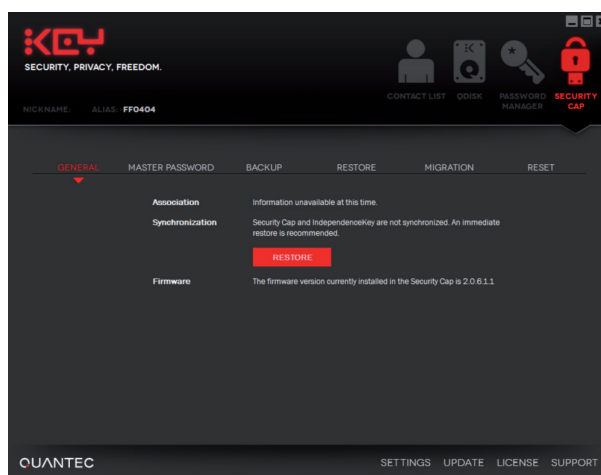
Nulla! I dati in esso contenuti sono totalmente crittografati e protetti dalla Master Password. Una volta perso è possibile acquistare un nuovo Security Cap e associarlo alla propria IndependenceKey. Da questo momento in poi la propria IndependenceKey riconoscerà solo ed esclusivamente il nuovo Security Cap.



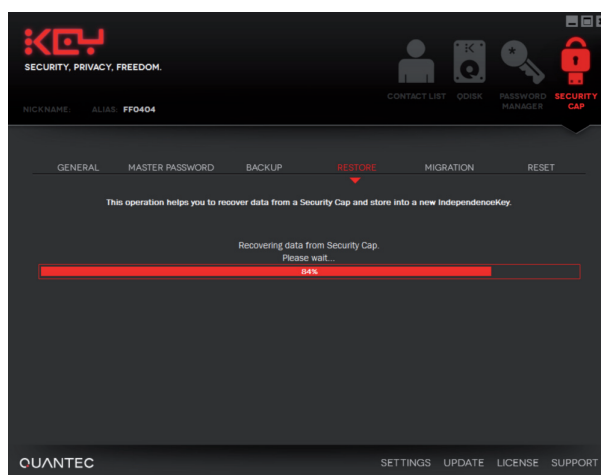
Utilizzo del Security Cap

RESTORE

Se si inserisce un Security Cap contenente già un proprio backup in una IndependenceKey nuova (o resettata alle condizioni di fabbrica), il software proporrà come unica scelta possibile quella di effettuare un restore dei dati presenti nel Security Cap all'interno della IndependenceKey.



Per questioni di sicurezza, onde poter procedere al restore, è necessario inserire la Master Password del proprio Security Cap. Questa procedura consente di recuperare tutti i dati relativi all'ultimo backup disponibile presente nel proprio Security Cap nel caso di smarrimento o furto della propria IndependenceKey. In questo caso è sufficiente acquistare una nuova IndependenceKey, inserire nella sua porta USB posteriore il proprio Security Cap e seguire la procedura a video. Una volta associato alla nuova IndependenceKey, il Security Cap funzionerà soltanto con quest'ultima e non più con la precedente.

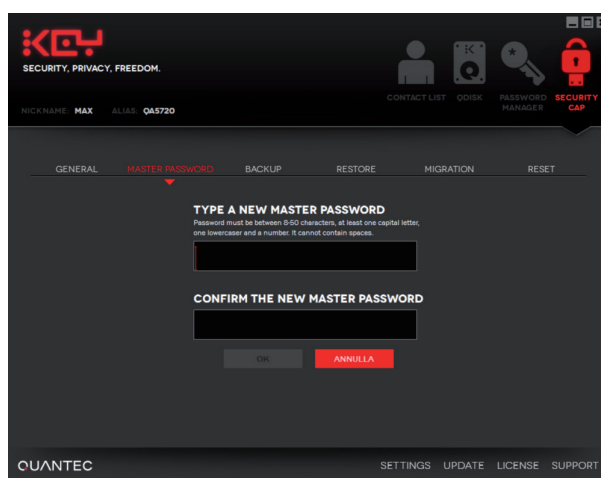


Si ricorda che il Security Cap deve essere sempre rimosso dalla propria IndependenceKey affinché quest'ultima possa essere utilizzata.

MODIFICA DELLA MASTER PASSWORD

Può accadere che la Master Password venga dimenticata. IndependenceKey è in grado di gestire anche questo evento nella massima sicurezza: **non è assolutamente necessario trascrivere la propria Master Password su supporti cartacei o altro!** Pensa a tutto il Security Cap.

In questo caso è necessario inserire il proprio Security Cap nella propria IndependenceKey; il dispositivo si sblocca e, tramite l'interfaccia utente, è possibile modificare agevolmente la propria Master Password. Da questo momento in poi la nuova Master Password è effettiva.



N.B.: In questo modo IndependenceKey viene automaticamente sbloccata dal proprio Security Cap: quando IndependenceKey viene inserita nel computer congiuntamente al proprio Security Cap, non viene richiesta la Master Password. Tuttavia, dato che il Security Cap è il dispositivo di sicurezza di backup dei dati crittografici, IndependenceKey non funzionerà fintantoché il Security Cap stesso non verrà rimosso.

BACKUP CONTINUI

Il Security Cap consente di ripristinare su una nuova IndependenceKey le chiavi crittografiche, i dati contenuti nel proprio Password Manager e i dati delle associazioni con altri utenti aggiornati all'ultimo backup effettuato. È evidente che se l'ultimo backup risale a un mese prima, la nuova IndependenceKey disporrà dei dati aggiornati a quella data. Se nel frattempo ci si è associati con nuovi utenti, queste associazioni non saranno presenti nel backup: sarà quindi necessario riassociarsi. Anche i dati del Password Manager non saranno aggiornati e così tutto il resto.

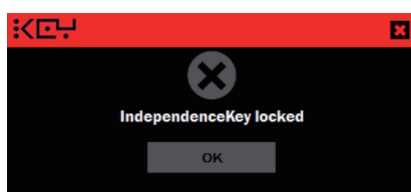
Per ovviare a questo potenziale problema, Quantec rende disponibile il servizio di Data Bank che esegue il backup continuo dei dati, sempre in maniera assolutamente riservata e protetta, 24 ore su 24. Ci si riferisca al capitolo successivo per i dettagli.



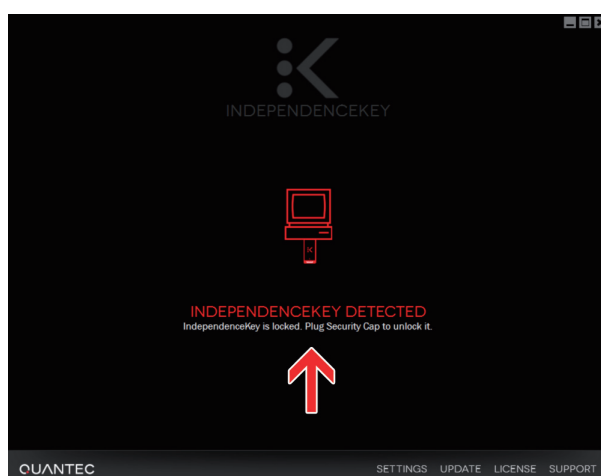
Utilizzo del Security Cap

SBLOCCO DI INDEPENDENCEKEY

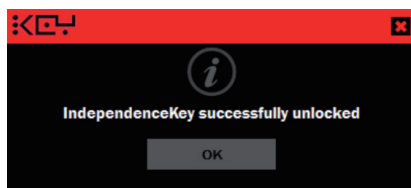
Come indicato nel primo capitolo relativo all'inizializzazione e come specificato nelle note tecniche a lato, la propria IndependenceKey è indissolubilmente associata con il proprio Security Cap. La Master Password è uno degli elementi chiave per poter utilizzare uno dei due dispositivi in maniera disgiunta. Quando si uniscono, non è più necessaria la Master Password ed è possibile modificarla. Un'altra funzione del Security Cap è quella di poter sbloccare l'IndependenceKey con la quale è associato nel caso in cui quest'ultima sia andata in blocco. IndependenceKey può andare in blocco se si supera il numero massimo di tentativi consecutivi di inserimento della Master Password, ovvero si digita una Master Password sbagliata per più di 5 volte consecutive.



IndependenceKey dispone di un meccanismo di protezione contro gli attacchi "a forza bruta" (brute force attack) e il blocco permette all'utente di rilevare se qualcuno ha tentato di accedere forzatamente alla propria IndependenceKey.



In caso di blocco basta inserire il Security Cap nell'IndependenceKey con cui è associato per ripristinarne immediatamente l'utilizzo.



Utilizzo del Data Bank



ASPETTI TECNICI



Il Data Bank è un servizio di protezione ulteriore, che si può aggiungere a quella già offerta dal Security Cap.

Come il Security Cap, il Data Bank permette di eseguire il backup delle chiavi crittografiche, dei segreti combinatori, delle associazioni con altri utenti e dei dati del Password Manager contenuti nella propria IndependenceKey.

Il Data Bank è stato realizzato per le persone che viaggiano a lungo e non hanno la possibilità di portare sempre con sé il proprio Security Cap, per coloro che temono di poter smarrire sia la propria IndependenceKey che il Security Cap, perdendo così l'accesso a tutti i dati protetti con IndependenceKey e per tutti quelli che hanno la necessità di disporre di dati riservati che devono essere accessibili anche a terzi (partner, soci, etc..) in casi particolari. Per venire incontro a tutte queste esigenze, il Data Bank consente di creare in ogni momento una IndependenceKey aggiornata con i dati crittografici necessari per accedere ai propri dati riservati.

Il Data Bank è un dispositivo equivalente come livello di sicurezza al Security Cap dal quale differisce per il colore (blu) e soprattutto per la logica di funzionamento.

Una volta sottoscritto il servizio, il Data Bank viene inviato all'utente il quale lo associa alla propria IndependenceKey. A differenza del Security Cap non deve essere periodicamente inserito nella IndependenceKey per eseguire i backup. Può essere, quindi, conservato in un posto sicuro e lasciato lì indefinitamente.

Ogni qualvolta IndependenceKey rileva un aggiornamento dei dati crittografici, di associazione o del Password Manager in essa contenuti, esegue un backup criptato hardware sui server di Quantec o sui server aziendali, in automatico (vedi la sezione tecnica a lato per i dettagli). Tale backup è archiviato in maniera ridondata sui server di Quantec, in territorio Svizzero, oppure può avvenire direttamente sui server aziendali ed è associato al numero di serie del proprio Data Bank. Il backup avviene in automatico nel momento in cui il computer in cui è inserita IndependenceKey è connesso a Internet.

In caso di smarrimento della propria IndependenceKey, è sufficiente ordinarne una nuova, inserire il proprio Data Bank nella porta USB posteriore della IndependenceKey e il gioco è fatto: non serve altro! Automaticamente, IndependenceKey recupera il backup correlato al Data Bank in essa inserito, lo invia al Data Bank che lo decripta e si riprogramma aggiornata all'ultima modifica apportata. Tutte le informazioni crittografiche, le associazioni con gli altri utenti e i dati del Password Manager vengono automaticamente ripristinati all'interno della nuova IndependenceKey.

La precedente IndependenceKey non sarà più utilizzabile e verrà automaticamente bloccata dai server Quantec non appena si collegherà a Internet. I dati in essa contenuti non sono accessibili se non si conosce la Master Password con cui essa è stata inizializzata.

Come funziona il Data Bank?

Quando il Data Bank viene inserito nella propria IndependenceKey, questo si associa indissolubilmente con essa come fa il Security Cap, ma in aggiunta scarica nella IndependenceKey una chiave crittografica specifica e segreta che solo quel Data Bank, sarà in grado di riutilizzare. La chiave viene memorizzata nel chip crittografico TPM protetto anche dai tentativi di accesso esterni. Tramite tale chiave crittografica, la propria IndependenceKey esegue un backup criptato dei dati crittografici in essa contenuti sui server di Quantec o sui server aziendali. I server ricevono tale insieme di byte per essi assolutamente incomprensibile in quanto non sono in possesso della chiave crittografica del Data Bank ma si limitano ad associarlo al numero di serie del Data Bank. La chiave crittografica del Data Bank viene generata localmente dal Data Bank stesso durante la fase di associazione con la propria IndependenceKey.

Il backup sui server Quantec è sicuro?

Per i motivi sopra espressi, i server Quantec archiviano un insieme di byte criptati, quindi incomprensibili a chiunque non in possesso delle chiavi crittografiche per decriptarli, correlati esclusivamente al numero di serie del Data Bank che è in grado di decriptarli. Non è possibile decriptare altrimenti tali dati in quanto protetti in AES 256 in hardware.

I server Quantec sono sicuri?

Quantec dispone di un proprio server cluster all'interno di un data center situato in Svizzera, specializzato in applicazioni mission-critical per il settore bancario e TLC. I server di Quantec sono protetti all'interno di un bunker sotterraneo e i dati in essi contenuti sono a loro volta giornalmente archiviati su altri sistemi, in backup. Tutti i backup realizzati tramite il Data Bank sono soggetti a backup costante e giornaliero su altri sistemi dislocati nel territorio svizzero.

È possibile eseguire il backup per conto proprio? Ad esempio sui server aziendali?

Per esigenze specifiche della propria clientela, Quantec consente al cliente di eseguire i backup ovunque desideri tramite un modulo software opzionale che è possibile installare su uno o più dei propri server aziendali dedicati. In questo modo l'archiviazione dei backup realizzati con il Data Bank e la versione Commander di IndependenceKey per applicazioni aziendali e governative mission-critical è garantita anche in particolari scenari di disaster recovery fisico (è possibile disporre, in automatico, di tutti i backup desiderati ovunque si voglia).



Keylogger e Master Password

ASPETTI TECNICI



Nel caso si tema che nel proprio PC sia presente un Keylogger è possibile inserire una tastiera USB direttamente nella porta USB posteriore di IndependenceKey e digitare direttamente la Master Password nel dispositivo.

A questo punto si può continuare a lavorare lasciando la tastiera inserita nella USB posteriore.

Questa funzionalità verrà rilasciata nel prossimo futuro tramite un upgrade del prodotto.

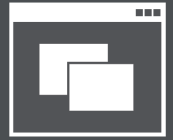
È tuttavia sempre possibile sbloccare la propria IndependenceKey inserendo il Security Cap con cui è stata inizializzata. Si ricorda che, in questo caso, occorre rimuovere il Security Cap dopo aver sbloccato IndependenceKey per poterla utilizzare.

Che cos'è un keylogger?

Il keylogger è un particolare malware informatico, ovvero un programma malevolo, che risiede nel computer all'insaputa dell'utente. Ha il compito di memorizzare tutti i tasti che vengono premuti dall'utente durante l'uso del computer, permettendo a terzi non autorizzati di comprendere cosa l'utente digiti, ovvero ricostruire email, testi e password.

Se si ritiene che il proprio computer possa essere soggetto ad attacchi di questo tipo, si può ricorrere a una tastiera USB esterna. Una soluzione semplice e immediata: basta inserire la tastiera nella porta USB host posteriore di IndependenceKey e digitare la Master Password. In questo caso nessun malware di alcun tipo sarà in grado di comprendere cosa venga digitato poiché IndependenceKey non esporrà la tastiera al computer fintantoché non verrà inserita la Master Password corretta. Prima di quel momento la tastiera non verrà rilevata dal computer, a livello hardware e quindi nessun malware sarà in grado di intercettarla. ***Una volta inserita la propria Master Password, IndependenceKey sbloccherà la tastiera in modo che quest'ultima possa essere utilizzata come di consueto.*** È anche possibile lasciarla inserita dietro la propria IndependenceKey.

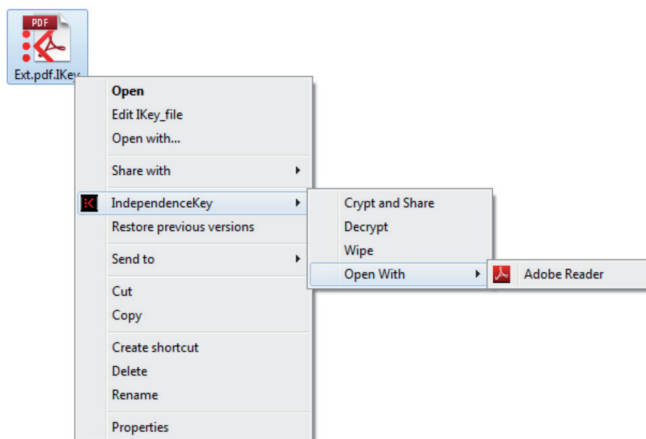
Se, tuttavia, il proprio computer fa parte di un domino aziendale, è amministrato in maniera coerente dall'IT Manager della propria azienda ed è dotato degli opportuni strumenti software necessari quali i moderni antivirus, l'evenienza di un evento del genere è abbastanza remota.



IndependenceKey utilizza un meccanismo semplice ed efficiente per abilitare le applicazioni autorizzate ad accedere automaticamente ai file criptati. In questo modo, l'accesso ai file criptati avviene senza dovere cambiare le proprie abitudini di lavoro e, nel contempo, **l'utente viene sempre avvisato quando un programma non autorizzato tenta di accedere a un file protetto.**

Quando si apre un file con il doppio click, IndependenceKey accede al file, verifica automaticamente i parametri necessari e richiama l'applicazione correlata. Ad esempio, se il file è un file di tipo “.docx” e sul computer è installato Microsoft Word, IndependenceKey eseguirà il programma Word, lavorando direttamente sul file criptato.

È comunque possibile aprire i file criptati anche con Wordpad o altri programmi ricorrendo all'opzione “Apri con” nel menù contestuale di IndependenceKey. Per far ciò è sufficiente cliccare sul file desiderato con il pulsante destro del mouse, scegliere il menù di “IndependenceKey” -> “Apri con” (“Open with”). Questo vale per tutti i programmi presenti nel computer e non solo per Word.



Tuttavia nel computer possono essere in esecuzione altri programmi che intendono accedere ai file criptati, come ad esempio un antivirus. In questo caso è bene abilitare l'antivirus all'apertura del file criptato perché, non facendolo, è possibile che quest'ultimo impedisca l'esecuzione del programma associato al file perché impossibilitato a comprenderne il contenuto.

Se un programma non abilitato richiede l'accesso a un file criptato è sempre l'utente a decidere se conferire tale accesso o meno, rispondendo sì o no al pop-up informativo che appare a video. Se si risponde di sì, il programma viene inserito in una speciale lista dei programmi abilitati accessibile tramite il menù “Impostazioni” (“Settings”) -> “Preferenze” (“Preferences”) -> “Applicazioni” (“Applications”).

Il “doppio click” di IndependenceKey

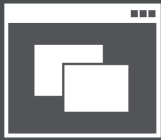
Una delle caratteristiche uniche e vincenti di IndependenceKey è la capacità di aprire e gestire i file criptati come se non fossero criptati. Proprio grazie a questa capacità, la presenza di IndependenceKey non richiede all'utente di modificare le proprie abitudini di lavoro. Tale funzione, correlata al classico “doppio click” sull'icona del file, è in realtà una funzione base di qualsiasi moderno sistema operativo.

Cosa succede quando si fa doppio click su un file? Il sistema operativo accede a una specifica area interna, il registro, e comprende quale tipo di applicazione è associata a tale file (di solito interpretando l'estensione del file). Se l'applicazione è nota e installata nel computer, la esegue indicandole di aprire il dato file, altrimenti riporta l'errore. In ogni caso è possibile ricorrere all'opzione “Apri con” (“Open with”), per poter aprire il file anche con applicazioni diverse da quella di “default” con la quale il file è associato.

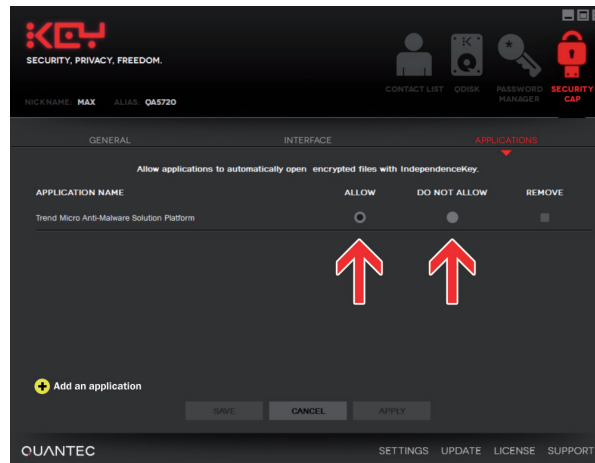
IndependenceKey opera al disotto del file system del sistema operativo, ovvero tra i dispositivi di storage e il file system stesso. Quando l'utente richiede di aprire un file con una data applicazione, questa inizia a richiedere al file system le varie parti del file ad essa necessarie. A questo punto entra in gioco IndependenceKey che, per conto dell'applicazione, accede al file e ne decripta solo le parti richieste inviandole all'applicazione. Viceversa, quando l'applicazione richiede di memorizzare nel file delle parti aggiornate, IndependenceKey crittografa i dati ricevuti e li memorizza nel file già criptato. Tutto avviene in tempo reale in maniera completamente invisibile per l'utente e per le applicazioni.

Affinché tutto questo possa avvenire l'applicazione deve essere autorizzata ad aprire il file. Tutte le applicazioni già installate nel proprio computer, sono autorizzate di default. Le applicazioni non autorizzate vengono gestite tramite un pop-up informativo in modo che sia sempre l'utente a decidere se conferire o meno a un'applicazione l'accesso a un dato file.

Se il proprio antivirus richiede l'accesso a un file, è opportuno conferirgli l'autorizzazione in modo che non blocchi poi, a sua volta, l'applicazione principale. Tuttavia, se un' applicazione sconosciuta richiede l'accesso a un file criptato è bene, prima di rispondere sì, comprendere di che applicazione si tratta. Se si risponde sì, IndependenceKey renderà disponibili in chiaro le parti del file richieste dall'applicazione. In questo modo l'utente ha il controllo totale sui propri file criptati. Generalmente, una volta installata IndependenceKey, è necessario al più conferire l'autorizzazione di accesso al proprio antivirus o software antimalware. Una volta concessa l'autorizzazione è sempre possibile rimuoverla in ogni momento tramite l'interfaccia utente.



Programmi e autorizzazioni



Tramite l'interfaccia è possibile abilitare, disabilitare oppure rimuovere un programma presente tra quelli abilitati.

Questa funzionalità è molto utile anche per quei programmi, come ambienti di sviluppo RAD, CAD/CAM, sistemi di authoring, etc.. che aprono più file contemporaneamente nel contesto di un progetto. In questo caso, occorre abilitare il programma specifico a operare direttamente sui file criptati da IndependenceKey.

Tramite il pulsante "Autorizza nuova applicazione" ("Authorize new application") è possibile aggiungere manualmente un'applicazione autorizzata ad accedere a un file protetto con IndependenceKey. Successivamente, per rimuoverla dalla lista delle applicazioni autorizzate basta selezionare l'opzione "Rimuovi" ("Remove") e premere il pulsante "Applica" ("Apply").

Si ricorda che IndependenceKey può abilitare un dato programma ad accedere a un file criptato facendo doppio click in Windows Explorer su tale file oppure aprendo il file tramite l'opzione "Apri con" ("Open with") nel menù contestuale sotto la voce "IndependenceKey" e non, generalmente, aprendo il file tramite le opzioni interne e specifiche del programma. L'abilitazione è un'operazione una-tantum.

Si consiglia di ricorrere ai dischi criptati QDisk di IndependenceKey se i programmi utilizzati devono lavorare su molti file contemporaneamente. In questi casi è la soluzione più efficiente.

Rimozione di IndependenceKey



IndependenceKey è un dispositivo in grado di crittografare dati, file, cartelle e dischi nonché flussi audio/video e VoIP in tempo reale. Se, mentre è in funzione, viene rimossa dal computer in cui è inserita, possono verificarsi errori nella crittografia dei file e nei dati in genere, esattamente come avviene con un dispositivo USB di storage se lo si rimuove dal computer mentre ci si stanno copiando sopra dei file. Nel caso di IndependenceKey, le operazioni crittografiche si interrompono.

Tuttavia, IndependenceKey è progettata per essere il più possibile sicura e a prova di errore (“failsafe”). Per questo motivo è in grado di gestire condizioni d'uso particolari come, ad esempio, la rimozione del proprio Security Cap mentre è in corso un backup o un restore: non accade nulla di particolare, reinserendo il Security Cap l'operazione ricomincia da dove era stata interrotta.

Anche se si rimuove IndependenceKey durante la fase di inizializzazione non succede nulla di irreparabile. In questo caso, una volta reinserita la propria IndependenceKey con il suo Security Cap, l'inizializzazione riprende da dove era stata interrotta.

Se invece IndependenceKey viene rimossa mentre sta crittografando un file si perderà il lavoro svolto: il file crittografato che si stava creando viene eliminato perché incompleto. In questo caso, se la funzione di “Autowiping” è abilitata, il file in chiaro non viene eliminato perché non è stato possibile crittografarlo completamente.

Nel caso si stia utilizzando un disco criptato (Qdisk) e si stiano copiando al suo interno dei file, smontando il disco (senza rimuovere IndependenceKey) il sistema prima termina le operazioni in corso e poi smonta il disco stesso. Se invece, durante questa operazione, si rimuove bruscamente IndependenceKey dal computer, i file copiati risulteranno corrotti esattamente come avviene con qualsiasi disco e dispositivo di mass storage quando lo si rimuove forzatamente mentre ci si stanno copiando sopra dei dati.

In tutti i casi **si consiglia sempre di eseguire la procedura di rimozione sicura di IndependenceKey cliccando sulla “K” in basso a destra nella system tray bar e scegliendo l'opzione > “Rimozione Sicura” (“Safe Remove”).**

In questo modo il dispositivo verifica se ci sono operazioni in corso e, nel caso, notifica all'utente la necessità di portarle a termine prima di rimuovere IndependenceKey. Se non ci sono operazioni in corso, IndependenceKey viene disattivata ed è possibile rimuoverla in tutta sicurezza. Il LED lampeggiante sul dispositivo si spegne a indicare che è possibile estrarla. Dopo essere stata disattivata per poterla utilizzare nuovamente è necessario estrarla e reinserirla nel computer.

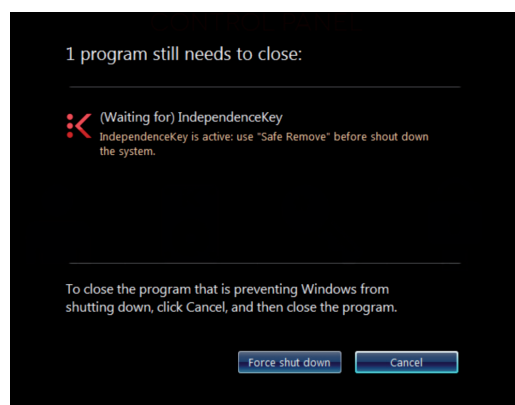


Se, invece, stai copiando dei file sui dischi protetti da IndependenceKey oppure hai dei file criptati aperti da qualche applicazione (ad esempio, un documento criptato aperto con Microsoft Word o un'altra applicazione), non sarà possibile estrarre IndependenceKey in maniera sicura. In questo caso l'interfaccia utente ti notificherà la necessità di chiudere i file protetti.

La stessa cosa accade se metti in stand-by (sospensione) o tenti di spegnere il tuo computer mentre IndependenceKey è attiva: in questo caso Windows notifica, nella lista dei programmi da chiudere, che IndependenceKey è operativa. È opportuno cliccare sul pulsante “Annulla” (“Cancel”), ritornare sul desktop, chiudere eventuali file criptati e dischi e, quindi, ripetere l'operazione in tutta sicurezza.

Più in generale, **è consigliabile eseguire la “Rimozione sicura” (“Safe Remove”) di IndependenceKey prima di mettere il computer in stand-by** sia tramite l'interfaccia di Windows, sia tramite i meccanismi automatici resi disponibili dall'hardware (ad esempio: chiudendo il display di un notebook o premendo il pulsante di sospensione del computer).

Al ripristino della sessione di lavoro dopo la sospensione, se la tua IndependenceKey è rimasta inserita nel computer, ti sarà richiesto di reinserire la Master Password onde sbloccarla e riprendere il lavoro.





Reset e migrazione

ASPETTI TECNICI



IndependenceKey è progettata per conservare al proprio interno, in massima sicurezza, i dati crittografici fondamentali per poter accedere ai file, dischi e contenuti criptati sia personali che condivisi con altri utenti. È inoltre progettata per **eseguire un backup e restore di tali dati sicuro e protetto, totalmente sotto il controllo dell'utente**. IndependenceKey memorizza al proprio interno tutte le chiavi crittografiche e i segreti combinatori che si vengono a creare man mano che viene utilizzata, a partire dalla sua inizializzazione, ivi inclusi i dati relativi alle associazioni con gli altri utenti. IndependenceKey memorizza anche tutti i dati del Password Manager e ne esegue il backup e restore sicuro.

RESET

È possibile resettare alle condizioni di fabbrica la propria IndependenceKey, ovvero eliminare tutti i segreti combinatori, le chiavi crittografiche e i dati del Password Manager presenti nel dispositivo seguendo la procedura di "Reset" tramite l'interfaccia utente.

ATTENZIONE: una volta che la propria IndependenceKey viene riportata ai valori di fabbrica, non sarà più possibile accedere ai dati precedentemente criptati, siano essi file, dischi o qualsiasi altro dato o informazione protetta con IndependenceKey.

Per procedere al reset assicurarsi che la propria connessione a Internet sia attiva. Inserire IndependenceKey nel computer insieme con il proprio Security Cap. Selezionare l'opzione -> "Reset" sull'interfaccia utente, nel menù relativo al Security Cap

Tramite i server Quantec la propria IndependenceKey verrà automaticamente riportata alle condizioni iniziali di fabbrica. Una volta avviata la procedura non è più possibile arrestarla.

MIGRAZIONE

La migrazione è una procedura complementare al reset e consente di spostare fisicamente, in completa autonomia, i dati crittografici presenti nella propria IndependenceKey all'interno di una nuova IndependenceKey. La migrazione consente di fare un upgrade della propria IndependenceKey a una nuova versione, oppure cambiarla con una nuova IndependenceKey.

Per procedere alla migrazione assicurarsi che la propria connessione a Internet sia attiva, inserire la vecchia IndependenceKey nel computer e sbloccarla. Inserire la nuova IndependenceKey nella porta USB posteriore della vecchia. Inserire il Security Cap della vecchia IndependenceKey nella porta USB posteriore della nuova IndependenceKey. Seguendo la procedura a video tramite l'interfaccia utente, tutti i dati crittografici presenti nella prima IndependenceKey insieme a quelli del Password Manager migreranno nella nuova IndependenceKey.

Il Security Cap della vecchia IndependenceKey viene associato univocamente alla nuova IndependenceKey, mentre la vecchia IndependenceKey viene resettata e riportata alle condizioni di fabbrica.

D'ora in poi è possibile utilizzare la nuova IndependenceKey con il Security Cap della vecchia IndependenceKey. Il Security Cap della nuova IndependenceKey, che non è stato inizializzato, va abbinato alla vecchia IndependenceKey che è stata resettata e portata alle condizioni di fabbrica durante la procedura di migrazione.

Per ogni domanda e necessità di chiarimento fare riferimento al supporto di IndependenceKey, integrato nell'interfaccia utente (vedi capitolo successivo).

Come sono protetti i segreti dentro IndependenceKey?

IndependenceKey contiene specifici chip dedicati alla crittografia, all'autenticazione e alla generazione e gestione sicura delle chiavi crittografiche. Tali chip, appartenenti alla piattaforma TPM (Trusted Platform Module), consentono non solo di generare e gestire tutti i segreti combinatori durante l'uso di IndependenceKey, ma anche di proteggerli in zone di memoria a loro volta sigillate, protette dall'accesso esterno da tentativi di analisi basati sulle correnti deboli e sulla derivazione del clock.

Cosa avviene con il Reset?

Resettando IndependenceKey si cancellano tutti i segreti presenti nei chip crittografici, eliminando tutte le chiavi crittografiche che sono state generate nel tempo, la chiave primaria dell'utente, i segreti combinatori relativi alle associazioni con altri utenti e così via fino ad arrivare ai dati contenuti nel Password Manager. **Tutto viene tutto cancellato in maniera sicura, blocco per blocco, a basso livello direttamente nell'hardware.** Una IndependenceKey resettata non è distinguibile da una IndependenceKey nuova di fabbrica dal punto di vista dei dati in essa contenuti.

Perché devo essere connesso a Internet?

Per resettare una IndependenceKey, Quantec richiede che il computer attraverso il quale avviene il reset sia connesso a Internet in modo da poterla bloccare all'interno del proprio data base.

La migrazione è sicura?

Tutti i processi crittografici di inizializzazione, di associazione, di backup e restore dei dispositivi sono realizzati a livello firmware all'interno dei dispositivi IndependenceKey e Security Cap stessi. In ogni istante sono interrompibili, anche in maniera forzata, estraendo, ad esempio, il Security Cap mentre si esegue un backup o un restore. Anche la migrazione avviene esclusivamente tra dispositivi IndependenceKey ed è totalmente a prova di errore ("failsafe"), ovvero IndependenceKey è in grado di recuperare ogni condizione di errore, ivi inclusa l'estrazione della nuova IndependenceKey dalla vecchia mentre la procedura è in corso.

Quando la migrazione è terminata, tutti i dati presenti nella vecchia IndependenceKey vengono trasferiti nella nuova e, quindi, cancellati per sempre nella vecchia IndependenceKey.



IndependenceKey è stata progettata per risultare sostanzialmente invisibile all'utilizzatore nella maggior parte delle attività quotidiane e dei servizi erogati.

Quantec ritiene che il supporto tecnico sia un elemento essenziale. Per questo motivo è stato integrato direttamente nell'interfaccia utente del software in dotazione con IndependenceKey.

Per rivolgersi al supporto tecnico basta aprire l'interfaccia utente, cliccare in basso a destra sul link "Assistenza" ("Support") e scegliere l'opzione "Assistenza Tecnica" ("Technical Support"). È possibile scrivere il proprio messaggio nella finestra che si apre. Premere "Invio" ("Send") ed esso verrà inviato immediatamente al supporto tecnico di Quantec.

È inoltre sempre possibile inviare un'email all'indirizzo **support@independencekey.com** o **support@quanteclab.com**, oppure aprire un ticket sul sito di IndependenceKey con il proprio account avendo cura di specificare il proprio Alias (riportato nell'interfaccia utente sotto il logo di IndependenceKey).

È possibile inviare suggerimenti e opinioni riguardo ai prodotti, all'interfaccia utente, all'ergonomia e alla fruibilità dei servizi erogati, così come idee e suggerimenti su futuri servizi desiderati. Per far questo, cliccare in basso a destra sul link "Assistenza" ("Support") nell'interfaccia utente e scegliere l'opzione "Suggerimenti" ("Suggestions"), indi seguire le opzioni proposte a video.

Per inviare le richieste è necessario essere connessi a Internet e disporre della propria IndependenceKey inserita e sbloccata nel computer.

ASPETTI TECNICI

Cosa succede quando invio una richiesta?

Il sistema di comunicazione di IndependenceKey con i server Quantec è crittografato a livello hardware dal dispositivo stesso. I server Quantec non accettano connessioni se queste non provengono da dispositivi IndependenceKey correttamente abilitati e inizializzati. È necessario disporre della propria IndependenceKey inserita e sbloccata nel proprio computer per poter accedere ai servizi on-line di IndependenceKey. Tuttavia, è possibile inviare le richieste di supporto e di assistenza anche senza disporre della propria IndependenceKey inserita nel computer.



Troubleshooting

PRIVACY E SICUREZZA

Qualcuno può recuperare i miei dati dopo che li ho cancellati?

Impossibile! IndependenceKey fa un wiping automatico di tutte le tracce in chiaro anche quando semplicemente cripta un file. Quando anche semplicemente lo cancelli tramite l'opzione "wipe" del menù, non sarà più recuperabile. In nessun modo. Inoltre quando apri un file criptato non viene decriptato in aree temporanee o altro! Il tutto avviene in memoria, in real time, e solo per le parti del file che l'applicazione richiede al sistema operativo, sia in lettura che in scrittura. L'integrità crittografica è poi garantita dall'engine a blocchi variabili di IndependenceKey. In questo modo, lavorando direttamente sui file criptati, non vi può essere fisicamente traccia di alcuna informazione in chiaro nel sistema.

Posso cedere la mia IndependenceKey ad un'altra persona? Esiste un reset per essere sicuro che l'altra persona non possa accedere ai miei dati?

Sì. Se passi ad un nuovo prodotto, una procedura guidata ti aiuta a creare una nuova IndependenceKey e resetta la tua vecchia IndependenceKey in modo che tu possa passarla ad altri senza pericoli. Puoi anche resettare direttamente IndependenceKey, in questo caso ricordati prima di decriptare i tuoi dati. Per eseguire il wipe totale della tua IndependenceKey è richiesto anche l'uso del tuo Security Cap.

IndependenceKey o il Security Cap possono subire manomissioni senza che io me ne renda conto?

No. Né a livello software né a livello hardware. Addirittura, quando si tenta di aprirlo a livello hardware, il prodotto si rompe.

Se anziché nel corpo di una email, scrivo il mio messaggio in un file, lo cripto e lo allego, posso sentirmi protetto?

Al 100%. Stiamo pensando anche ad un tool software per lavorare direttamente con Outlook e proteggere anche tutta l'e-mail, ma per ora la procedura che hai indicato è l'unica protetta al 100%.

Ma le chiavi di crittografia chi le decide?

Le chiavi di crittografia vengono generate in hardware della IndependenceKey e sono tutte una diversa dall'altra. La Master Password è solo uno degli elementi che concorrono all'accesso delle chiavi crittografiche. Nessuno le può conoscere, né tu né le persone con cui vuoi condividere i documenti: l'unico modo che hanno per aprire i documenti è che siano associati a te tramite la loro IndependenceKey personale.

È possibile intercettare le comunicazioni tra Security Cap e IndependenceKey, tra IndependenceKey e computer o tra diverse IndependenceKey che comunicano?

No. Il Security Cap e IndependenceKey (ma vale anche tra IndependenceKey diverse) sono infatti associati 1:1 in modalità hardware: viene stabilito un canale criptato rendendo assolutamente sicura ogni comunicazione. Ciò consente di evitare ogni tipo di attacco ("Man in the Middle", "Replay Attack", etc..). Le comunicazioni tra IndependenceKey e computer anch'esse criptate con chiavi variabili di sessione in sessione.

E se ho un Malware o un Trojan nel computer può rilevare la Master Password?

Se la digiti direttamente dalla tastiera collegata al computer e tale trojan è un "Key Logger", sì. Ma c'è un modo per non correre alcun pericolo se ritieni di avere software dannosi nel computer (o usi un computer non tuo, etc.): ti è sufficiente inserire una tastiera USB direttamente dietro la IndependenceKey. Digiti la tua Master Password e sblocchi la chiave senza passare per il PC!

INIZIALIZZAZIONE E UTILIZZO

Come faccio ad inizializzare la mia IndependenceKey?

Dopo aver installato il software che puoi scaricare dal sito web, la prima volta basterà inserirla nella porta USB del computer e seguire la procedura guidata. In seguito, dovrai semplicemente inserirla nella porta USB del computer e sbloccarla con la tua Master Password scelta in precedenza. Nell'area di download trovi il manuale che spiega tutto ciò che puoi fare con la tua IndependenceKey.

Inserisco IndependenceKey ma non succede nulla, cosa devo fare?

IndependenceKey funziona su computer x86 dotati di sistema operativo Microsoft Windows, in differenti versioni: XP SP3, Vista, Windows 7 sia a 32 che a 64 bit. Probabilmente i requisiti minimi di sistema non sono rispettati. Le IndependenceKey sono tutte testate al 100% prima di essere inviate. Può tuttavia succedere che durante la spedizione accada qualcosa fuori dal nostro controllo e che venga, quindi, danneggiata. In questo caso, devi rivolgerti al distributore dove l'hai acquistata o aprire un ticket tramite il servizio di assistenza di IndependenceKey per poi concordare la procedura per far valere la garanzia.

IndependenceKey alle volte sembra molto calda. È normale?

Può accadere durante un uso intenso del dispositivo. Non dimenticare che non si tratta di un normale "chiavetta USB" ma di un computer embedded ad altissime prestazioni. IndependenceKey contiene, in poco più di 45x25 mm tutta l'elettronica che è presente nei più moderni computer e smartphone. Tutti dispositivi che scaldano. Certamente, le possibilità di dissipare il calore di IndependenceKey sono ridotte a causa delle sue piccolissime dimensioni e quindi il prodotto sembra essere più caldo. Il contenitore in metallo aiuta a raffreddarlo internamente a discapito della temperatura esterna. Tutti i parametri operativi sono largamente sotto le soglie di funzionamento e non è un difetto del prodotto.

Voglio acquistare una nuova IndependenceKey, devo decriptare e ri-cryptare tutti i documenti?

No. Devi seguire l'apposita procedura di migrazione per sostituire la vecchia IndependenceKey con la nuova. Terminata la procedura, la nuova IndependenceKey è immediatamente operativa, mentre quella vecchia è resettata e puoi darla ad altre persone, amici, colleghi e familiari.

Posso salvare dei file all'interno di IndependenceKey?

Nella versione dotata di memoria interna, sì. Nelle altre, no. All'interno di IndependenceKey vengono sì salvati dei dati, ma sono le chiavi di crittografia e le informazioni riservate. Nella versione con memoria interna (in funzione delle varie capacità disponibili), IndependenceKey è anche una velocissima "chiavetta USB criptata" di storage con due vantaggi: sia la velocità, sia il backup sul computer locale dei dati criptati ivi contenuti.

Posso usare più di una IndependenceKey sullo stesso computer?

Certamente. Attenzione però: sono IndependenceKey di utenti diversi quindi i file criptati da una IndependenceKey non saranno visibili alla seconda IndependenceKey a meno che le due IndependenceKey non siano associate ed i file condivisi.

Posso bloccare temporaneamente un contatto o devo cancellarlo per poi associarmi di nuovo?

I contatti che sono nella tua lista non possono aprire o vedere nulla, a meno che non sia tu ad estendere a questi utenti i diritti di accesso a file, cartelle e dischi. Bloccarli, quindi, non ha senso, a meno delle risorse condivise su server e sistemi Cloud aziendali dove, rimuovendo un dato utente da un file o da un disco questi non potrà più accedervi. I file che, chiaramente, sono stati invece già inviati per email o altri sistemi agli altri utenti e che non sono più da te raggiungibili, non possono essere più bloccati.

Se ho creato un file e ne ho esteso i diritti a 3 utenti, questi possono a loro volta estenderne i diritti ad altri loro utenti?

No! IndependenceKey utilizza il concetto di "owner". L'utente che crea il file crittografato è colui che può, in qualsiasi momento, estenderne o ridurne i diritti di accesso ad altri utenti. Quest'ultimi, non possono farlo.

Ho estratto IndependenceKey mentre era in funzione, ho combinato un danno?

Dipende dal tipo di operazione che era in corso. Per tutte le operazioni di inizializzazione, associazione con altri utenti, back-up, restore e migrazione non c'è alcun problema. Sono tutte operazioni che IndependenceKey esegue implicitamente in maniera assolutamente sicura anche in questi casi. Nel caso tu stessi criptando uno o più file, i file per i quali non è terminata la crittografia rimangono in chiaro. Se stavi lavorando su di un file criptato (ad, esempio, un documento Word) corri il rischio di perdere le ultime modifiche o, peggio, il file stesso. Nel caso tu stessi scrivendo sui dischi criptati (ad esempio, copiando file di grande dimensione o altro), molto probabilmente avrai perso il file come avviene con qualsiasi dispositivo di mass-storage se viene rimosso durante il suo utilizzo. Ti consigliamo di eseguire sempre la "Rimozione Sicura" di IndependenceKey cliccando sulla "K" in basso a destra, vicino all'orologio, prima di estrarla dal tuo computer.

Come devo rimuovere IndependenceKey?

Prima di rimuovere IndependenceKey, occorre effettuare la "Rimozione Sicura" dal menù in basso a destra nella system tray bar cliccando sopra la "K" rossa. Se, tuttavia, non si effettua l'unmount e non ci sono attività in corso, generalmente non accade nulla. È, comunque molto meglio effettuare sempre la rimozione sicura perché, semmai ci fossero attività in corso, allora ne verresti informato. Tale informazione viene riportata anche nel caso in cui effettui lo spegnimento del computer senza aver prima rimosso correttamente IndependenceKey.

Posso caricare i dati criptati con IndependenceKey su Dropbox, Skydrive, Power Folder, Wuala, Carbonite, etc.?

IndependenceKey è perfetta per questi utilizzi. Nessuno può più accedere alle tue informazioni e puoi utilizzare i servizi Cloud alla perfezione. Attenzione: ricorda di rispettare i termini e condizioni anche di chi ti offre il servizio Cloud.

Qual è la dimensione massima dei file che posso criptare?

Dal punto di vista delle dimensioni, IndependenceKey non pone alcun limite. Anzi, più sono grandi e più con IndependenceKey sperimenterai una incredibile velocità di crittografia e di sincronizzazione con il Cloud. Negli approfondimenti tecnici del manuale trovi maggiori dettagli.

Posso condividere i file tramite il Cloud?

Certamente. Ricorda però che non ti è sufficiente condividere l'accesso allo spazio Cloud: anche le IndependenceKey degli utenti devono essere associate per poter condividere i documenti, file e dischi ai quali si vuole offrire accesso.

IndependenceKey può proteggermi anche sui social network?

Nei Social Network sei tu che decidi di condividere pubblicamente le tue informazioni. Puoi criptare file e scambiarli con altri utenti / amici utilizzando i Social Network come strumento per passare e/o pubblicare informazioni riservate, ma sempre nel rispetto dei termini e condizioni.



Troubleshooting

SECURITY CAP

È necessario l'uso del Security Cap?

Ci hai mai pensato? Qualunque cosa tu faccia in Internet, c'è sempre qualcuno che conosce la tua "password di recovery" dei dati. Con il rivoluzionario Security Cap abbiamo finalmente risolto il problema. Tutto è in mano tua. È dotato anch'esso di chip di autenticazione crittografico, engine crittografico hardware e memoria in grado di fungere da sistema di backup sicuro e affidabile dei dati contenuti in IndependenceKey: delle chiavi crittografiche e delle associazioni con gli altri utenti, per ripristinare il tutto in caso di perdita o furto della tua IndependenceKey o, addirittura, amnesia. Questa soluzione brevettata apre una nuova era nella sicurezza individuale e delle aziende.

Ogni quanto lo devo collegare alla mia IndependenceKey per fare il backup?

Dipende da quanto utilizzi la tua IndependenceKey. Se la usi quotidianamente con diversi utenti, ti consigliamo di fare un backup frequentemente. Se la usi di meno, puoi farlo con minor frequenza. Quando la usi e, soprattutto, ti associ con nuovi utenti generi delle chiavi di crittografia, se non fai il backup e perdi la tua IndependenceKey puoi perdere l'accesso agli ultimi documenti che hai ricevuto da altri utenti. L'operazione è comunque talmente semplice e rapida da poter essere effettuata frequentemente.

E se perdo il Security Cap che cosa succede?

Tranquillo, non hai perso i dati. Ne puoi acquistare un altro e con la tua IndependenceKey e la tua Master Password puoi creare un nuovo Security Cap. È necessario avere sempre due elementi: se perdi la IndependenceKey, ti servono il Security Cap e la Master Password. se perdi il Security Cap: ti servono la IndependenceKey e la Master Password. dimentichi la Master Password: ti servono la IndependenceKey ed il Security Cap.

Quindi se rubano la mia IndependenceKey con il Security Cap possono decriptare i miei dati?

Sì. Per questo non dovresti tenerli insieme: più o meno come se ti rubassero Bancomat e PIN. Vanno tenuti separati.

E chi entra in possesso del mio Security Cap può aprire i miei file?

No. Entra in possesso di un oggetto che non è in grado di utilizzare, né ispezionare per estrarne i dati in chiaro. È sempre necessaria anche la Master Password.

Ho perso IndependenceKey e ho davvero bisogno di aprire i file criptati, ma la nuova IndependenceKey che ho ordinato non arriva prima della prossima settimana: cosa posso fare?

Non si può fare nulla. Per la tua sicurezza devi attendere il nuovo prodotto ed effettuare il restore dei dati.

È saltata la corrente mentre facevo il backup nel Security Cap, IndependenceKey funziona ancora? Devo fare un nuovo backup?

Sì. IndependenceKey è progettata per resistere anche a questo tipo di inconvenienti. Controlla sempre che i processi avviati siano conclusi.

ASSOCIAZIONE E CONDIVISIONE

Come avviene l'associazione?

Ci sono due modalità: FISICA: inserisci la chiave dell'utente con cui ti vuoi associare nella porta USB posteriore tua IndependenceKey. A questo punto segui le istruzioni. REMOTA: puoi associarti con utenti remoti, utilizzando l'apposito Alias univoco di ogni chiave (presente nel chip crittografico di IndependenceKey).

Se mi associo con qualcuno significa che può vedere/aprire i miei file o cartelle?

No. Puoi associarti con chiunque in totale sicurezza. Associarsi significa solo che da quel momento in poi puoi consentire ad una persona l'accesso ad uno specifico file, cartella o disco. Puoi associarti con un cliente, un fornitore, un collega, un amico, un familiare condividendo solo i file che desideri con le persone che desideri. L'associazione crea una chiave crittografica univoca ed universale tra te e l'utente con cui ti sei associato. Tramite tale chiave puoi successivamente estendere i diritti di accesso a file, cartelle e dischi. L'utente potrà accedere sempre e solo a ciò a cui tu l'autorizzi, gli altri file, cartelle e dischi sono al sicuro.

Se un utente al quale sono già associato mi manda un file, devo decriptarlo per aprirlo o devo salvarlo in una apposita area di memoria?

No. Puoi salvarlo dove preferisci mantenendolo criptato. Con IndependenceKey inserita e sbloccata (tramite la tua Master Password) apri il file con un semplice doppio click e ci lavori come hai sempre fatto. Viene decriptato in real time solo ed esclusivamente in memoria quello che serve e non c'è bisogno di farne una copia in chiaro sul tuo PC. Ovviamente, con IndependenceKey disinserita nessuno può aprire né i tuoi documenti, né quelli che altri utenti di IndependenceKey ti hanno inviato.

DATA BANK

Cosa devo fare quando ricevo il Data Bank?

Lo inserisci nella porta USB posteriore della tua IndependenceKey e lo metti in un luogo sicuro. Fine. Se vuoi, continui a fare i backup periodici con il tuo Security Cap, sapendo che il Data Bank ti regala una sicurezza in più 24 ore su 24.

Con il Data Bank associato dove vengono salvate le informazioni e quali informazioni?

Le informazioni salvate sono tutte quelle generate dalla IndependenceKey e quindi le chiavi di crittografia e le associazioni. Queste informazioni vengono crittate in hardware tramite la chiave crittografica univoca del Data Bank e, quando IndependenceKey è connessa ad Internet, vengono inviate in forma criptata ai server di Quantec. Nel caso in cui rubino la tua IndependenceKey, e contemporaneamente tu perda il Security Cap, con il Data Bank puoi ricostruire il tutto e non perdere alcuna informazione.

Quantec può aprire il file di backup che riceve?

In nessun modo. Per noi non ha alcun significato: sono dati criptati in hardware AES 256 ad alta entropia e senza alcun senso.



Appendice tecnica

INSTALLAZIONE DEL SOFTWARE IN WINDOWS XP

Per installare il software di IndependenceKey in Windows XP è necessario che il sistema operativo sia, prima di tutto, aggiornato alla versione Service Pack 3. È questo un requisito minimo fondamentale per il corretto funzionamento del software stesso.

Il software di IndependenceKey ed i suoi driver sono firmati digitalmente con un certificato emesso da una Certification Authority accreditata. Tale certificato (Microsoft Authenticode) consente di verificare, sin dall'avvio del setup, la genuinità del software grazie alla firma digitale di tutti i componenti chiave del programma. In Windows XP tale certificato non viene riconosciuto ed è necessario eseguire alcune fasi a mano. Negli altri sistemi operativi supportati, invece, avviene tutto in automatico senza alcun intervento dell'utente.

All'atto dell'avvio del setup in Windows XP SP3 può essere, pertanto, visualizzata la schermata seguente. In questo caso, premere il pulsante "Continua" ("Continue Anyway") per procedere. N.B. Il setup può impiegare anche alcuni minuti: non interromperlo.



Dopo aver installato il setup, riavviato il computer ed inserita IndependenceKey appare la seguente notifica nella system tray bar in basso a destra:



A questo punto nelle successive due schermate occorre selezionare la prima opzione disponibile e procedere cliccando su "Next":



Foto 1

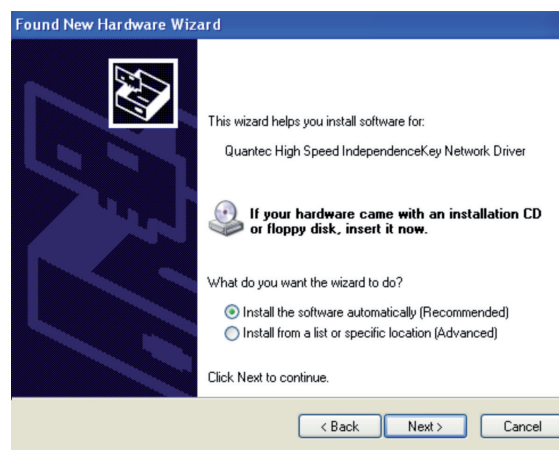


Foto 2

Windows XP rileverà automaticamente il driver corretto per il dispositivo IndependenceKey (foto 1 e 2) e, nella successiva schermata (foto 3), occorre premere il pulsante “Continua” (“Continue Anyway”) per procedere.

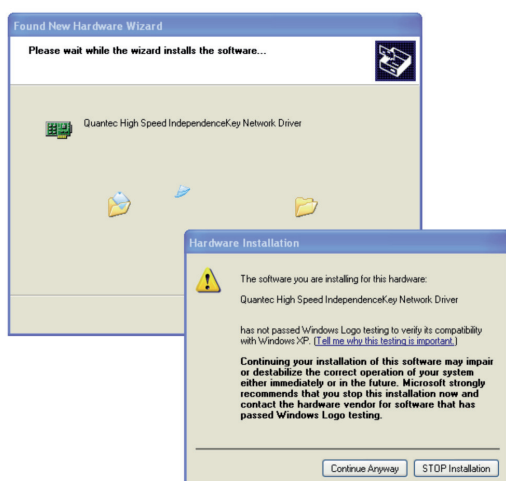


Foto 3

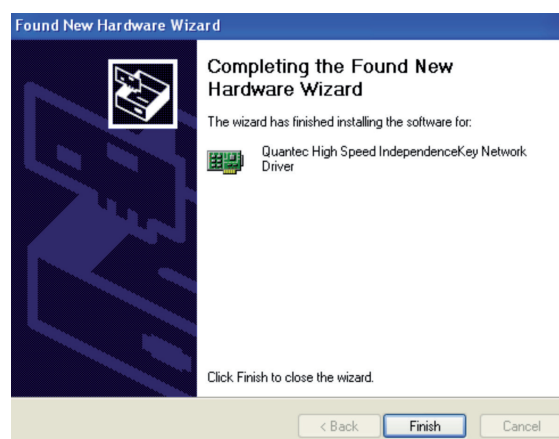


Foto 4

A questo punto il driver di IndependenceKey è stato installato e si può procedere cliccando sul pulsante “Finish” (foto 4).

Termini e condizioni sull'uso del software

QUANTEC SA TERMINI E CONDIZIONI DELLA LICENZA SOFTWARE

IMPORTANTE: L'UTILIZZO DI INDEPENDENCEKEY VINCOLA L'UTENTE AI SEGUENTI TERMINI E CONDIZIONI

SI INVITA A LEGGERE ATTENTAMENTE I PRESENTI TERMINI E CONDIZIONI PRIMA DI UTILIZZARE IL DISPOSITIVO INDEPENDENCEKEY O DI SCARICARE IL SOFTWARE O L'AGGIORNAMENTO SOFTWARE CHE ACCOMPAGNA QUESTA LICENZA. Con l'utilizzo di IndependenceKey o scaricando il software, accettate i termini e le condizioni della presente Licenza. Qualora non riteniate di accettare le condizioni e i termini seguenti, vi preghiamo di non utilizzare il dispositivo e non scaricare il software o suoi aggiornamenti.

1. TERMINOLOGIA E RIFERIMENTI

Prodotto: l'insieme dell'hardware e del software che compongono IndependenceKey.

Utente: la persona fisica o giuridica che utilizza il prodotto.

Software: il Software originale e gli Aggiornamenti Software;

Aggiornamenti Software: aggiornamenti del Software scaricabili dal sito Web o da Internet in generale, ivi inclusi gli aggiornamenti automatici inviati dai server Quantec.

IndependenceKey o IKEY: si riferisce generalmente al Prodotto.

Dati: i contenuti, la documentazione, le interfacce, e tutti i dati forniti da Quantec con IndependenceKey, così come quelli aggiornati o sostituiti dalle funzionalità aggiunte, sia su memoria di sola lettura, ovvero su altri supporti o in altra forma.

Security Cap: il dispositivo di back-up e restore di IndependenceKey

Servizi: le funzionalità messe a disposizione del Prodotto.

Garanzia Hardware: la garanzia di cui al documento "Garanzia Hardware" che è da ritenersi parte integrante e vincolante dei Termini e Condizioni.

Privacy: non viene trattata nei seguenti Termini e Condizioni ma nel documento "Privacy" che è da ritenersi parte integrante e vincolante dei Termini e Condizioni.

2. RESTRIZIONI ED USI CONSENTITI DI INDEPENDENCEKEY

IndependenceKey può essere utilizzata per criptare e decrittare file, cartelle, creare dischi criptati e criptare materiale in genere, condividere con terzi il materiale crittografato, caricare il materiale crittografato nel Cloud e sui server aziendali dell'Utente. IndependenceKey consente anche di criptare e decrittare in tempo reale flussi di dati (stream) digitali siano essi di tipo audio o audio/video ed effettuare, tramite opportune estensioni opzionali, anche telefonate VoIP non accessibili da parte di terzi indesiderati, nonché di firmare digitalmente file dati di ogni tipo e genere e di verificarne l'integrità strutturale, ovvero che non siano stati manomessi e/o modificati.

L'Utente accetta espressamente quanto segue:

1. L'utilizzo di IndependenceKey è limitato a materiale di cui l'Utente detenga il copyright, o non protetto da copyright, e che comunque non possa arrecare danno alla pubblica sicurezza o a terze parti in genere, ovvero non sia contrario a norme di legge.
2. Non potendo Quantec in nessun modo accedere o decrittografare il materiale dell'Utente, lo stesso con l'acquisto del Prodotto si impegna ad ottemperare senza riserve ad ogni richiesta, invito, ordine o ingiunzione emessi da qualsivoglia autorità in relazione al materiale medesimo, affinché Quantec sia esentata da ogni incombente e onere al riguardo.
3. Qualora utilizzi servizi Cloud o di File Transfer o qualunque altro servizio Internet, l'Utente si impegna a rispettare i termini e condizioni del fornitore del servizio, in modo da esentare Quantec da ogni incombente e onere al riguardo.
4. Archiviando i propri contenuti (file, dati e informazioni digitali) su IndependenceKey (versione con memoria di storage interna), ne esegue periodicamente una copia di back-up in altro dispositivo di mass storage. (In alternativa, quando disponibile, può utilizzare il plug-in software opzionale di IndependenceKey per il back-up automatico dei dati contenuti nella memoria di mass storage interna di IndependenceKey sul computer al quale è connesso il dispositivo stesso).
5. L'Utente si impegna ad utilizzare il Prodotto, il Software, e i Servizi secondo i termini della licenza concessa da Quantec ed in conformità a tutte le leggi applicabili, comprese la legislazione locale del paese o della regione in cui risiede o in cui acquista il prodotto o in cui scarica il Software o utilizza il Software e i Servizi.
6. L'Utente rispetterà fedelmente quanto al seguente paragrafo "Esportazione controllata"
7. L'utilizzo improprio è sotto l'esclusiva responsabilità dell'Utente.

3. LA LICENZA SOFTWARE.

1. Quantec concede all'Utente una licenza personale, limitata, non trasferibile e non esclusiva per l'utilizzo del Software e dei Dati, su uno o più computer di proprietà dell'Utente (la "Licenza"). La Licenza include altresì la facoltà di scaricare gli Aggiornamenti Software resi eventualmente disponibili da Quantec.
2. I Termini e Condizioni della Licenza regolano l'utilizzo dei Servizi e del Software, inclusi gli Aggiornamenti Software eventualmente forniti e/o resi disponibili da Quantec per la sostituzione e/o l'integrazione del Software, salvo che tali aggiornamenti siano regolati da licenza separata, nel qual caso si applicheranno termini e condizioni di quest'ultima.
3. Quantec è unica proprietaria del Software e si riserva tutti i diritti non espressamente accordati all'Utente con la Licenza.

4. LIMITAZIONI DELLA LICENZA SOFTWARE

1. Gli Aggiornamenti Software scaricati dall'Utente possono essere riprodotti in copia per soli scopi di backup e purché la copia riporti tutte le informazioni relative ai diritti d'autore o altri diritti di proprietà contenute nell'originale.
2. La Licenza non concede alcun diritto relativo all'utilizzo delle interfacce di proprietà di Quantec né di altre proprietà intellettuali per la fabbricazione, lo sviluppo, il design, la concessione in licenza o la distribuzione di dispositivi e accessori di terze parti né di applicazioni di terze parti da utilizzare con i dispositivi.
3. Non è consentito copiare, modificare, creare opere derivate del codice sorgente, decodificare, disassemblare o tentare in altro modo di scoprire tale codice, vendere, trasferire, concedere in sublicenza, dare in pegno o altrimenti trasferire qualsiasi diritto relativo al Software, a meno che tale attività non sia espressamente permessa o richiesta dalla legge o sia stata espressamente autorizzata da Quantec per iscritto. L'Utente si impegna dunque a non compiere nessuna delle predette azioni e riconosce ed accetta che il compimento, anche in termini di mero tentativo, di ciascuna di esse integra una violazione dei diritti di proprietà intellettuale ed industriale di Quantec.

5. TRASFERIMENTO

In deroga alla previsione di cui al punto 4 del paragrafo che precede, l'Utente può trasferire in maniera permanente tutti i diritti relativi al Software a terzi, in caso di trasferimento di proprietà di IndependenceKey, a condizione che:

1. il trasferimento riguardi il dispositivo IndependenceKey e tutti i componenti, inclusi il Software, i supporti originali, il materiale stampato e la Licenza;
2. l'Utente provveda ad eseguire il "reset" del dispositivo IndependenceKey e del Security Cap ad esso associato seguendo la procedura prevista nel software, ovvero mediante connessione internet. In tal modo i chip crittografici del dispositivo possono essere completamente cancellati ed entrambi i dispositivi riportati alle condizioni di fabbrica;
3. non venga conservata nessuna copia parziale o totale del Software, comprese eventuali copie memorizzate su computer o su altro dispositivo IndependenceKey di archiviazione dati;
4. la parte ricevente il Software legga e accetti i termini e le condizioni della Licenza e dell'eventuale licenza separata per gli Aggiornamenti Software.

6. CONSENSO ALL'UTILIZZO DI DATI

1. L'Utente accetta e riconosce che Quantec possa raccogliere, conservare, processare e utilizzare informazioni di diagnosi, utilizzo, tecniche, e altre informazioni ad esse collegate, in particolare (ma non esclusivamente) informazioni relative al dispositivo IndependenceKey, al computer, al Software di sistema e applicativo nonché alle periferiche in uso. Questi dati verranno raccolti da Quantec periodicamente per consentire ed agevolare la preparazione e la fornitura di aggiornamenti, supporto tecnico e altri servizi relativi al Software e per verificare la conformità ai termini e alle condizioni della Licenza. Quantec utilizzerà tali dati in misura e forma tale che non sia possibile scoprire l'identità della persona a cui appartengono, al solo scopo di fornire e migliorare i prodotti e servizi forniti. Per consentire ai partner e agli sviluppatori terze parti di Quantec di migliorare il proprio software, hardware e i servizi destinati all'utilizzo con i prodotti forniti, Quantec potrà inoltrare a tali partner e sviluppatori terze parti un sottoinsieme di informazioni di diagnosi importanti per il loro software, hardware e/o servizi, così come informazioni di diagnosi, in misura e forma tale che non sia possibile identificarvi personalmente.
2. I dati verranno trattati in ogni momento conformemente alla politica di tutela della privacy di Quantec, integrata come riferimento alla Licenza e consultabile su <http://www.independencekey.com/blog/privacy/>.

7. USO DEI SERVIZI

1. L'Utente riconosce e accetta che i Servizi ed il Software contengano informazioni proprietarie e riservate, di esclusiva proprietà di Quantec e protette dalle leggi applicabili in materia di proprietà intellettuale e da ogni altra norma - di legge o non - applicabile, ivi compresa, a titolo esemplificativo ma non esaustivo, la normativa in materia di copyright.
2. L'Utente accetta di non modificare, affittare, locare, concedere in leasing, noleggiare, vendere o distribuire, in tutto o in parte, i Servizi o il Software e di non creare opere derivate basate sui contenuti proprietari dei Servizi e del Software, a meno di specifica ed espressa autorizzazione rilasciata da Quantec per iscritto.
3. L'Utente accetta di non utilizzare i Servizi in modi non consentiti, compreso, a titolo esemplificativo ma non esaustivo, l'uso dei Servizi per la trasmissione di trojan, worm, virus informatici o altro malware.
4. L'Utente accetta di non utilizzare i Servizi in modo alcuno per molestare, perseguire, abusare, diffamare, minacciare, infrangere o violare in altra forma i diritti di terzi.
5. Quantec non è in alcun modo responsabile degli utilizzi non consentiti o posti in essere dall'Utente in danno di terzi, così come delle relative conseguenze, ivi comprese, a titolo esemplificativo, molestie, violazioni, diffamazioni, minacce, messaggi offensivi o illegali.
6. Quantec non garantisce che gli Aggiornamenti Software dalla medesima forniti e/o resi disponibili includano tutte le funzionalità esistenti nel software o le nuove funzionalità fornite da Quantec per altri o più recenti modelli di IndependenceKey.
7. Quantec non risponde dell'adeguatezza di servizi e materiali di terze parti cui l'Utente abbia eventualmente accesso utilizzando IndependenceKey.
8. Quantec si riserva il diritto di modificare, sospendere, interrompere o disabilitare l'accesso ad uno/alcuni/tutti i Servizi, così come di limitarne l'utilizzo e/o l'accessibilità in qualsiasi momento e di volta in volta, con o senza preavviso. L'Utente accetta che in ogni caso Quantec non sarà ritenuta responsabile nei propri confronti o di qualsiasi terza parte per dette modifiche, sospensioni e interruzioni dei Servizi.

8. REVOCA DELLA LICENZA

In caso di mancato rispetto anche di una sola delle clausole di cui ai Termini e Condizioni della Licenza, quest'ultima s'intenderà immediatamente ed automaticamente revocata senza necessità di alcun preavviso da parte di Quantec, con conseguente venir meno dei diritti con la stessa accordati all'Utente e relativo obbligo di cessazione immediata dell'utilizzo del Software e dei Servizi.

In caso di inosservanza dei Termini e Condizioni della Licenza, Quantec si riserva il diritto in ogni momento e senza preavviso alcuno di disattivare tutte le installazioni del Software effettuate dall'Utente nonché il/i dispositivo/i IndependenceKey da egli utilizzato/i.

Le responsabilità e le restrizioni poste a carico dell'Utente permangono anche a seguito della revoca della Licenza.

9. CLAUSOLA ESONERATIVA DI ALTRE GARANZIE

L'Utente dichiara di riconoscere ed accettare quanto segue:

1. nei limiti consentiti dalla legge applicabile, l'uso del Prodotto e dei Servizi rimane ad esclusivo rischio dell'Utente, anche in termini di qualità, precisione, prestazioni e impiego soddisfacente. I Servizi vengono forniti nello stato in cui si trovano ed in base alla loro disponibilità. Quantec non riconosce espressamente alcuna garanzia e/o condizione di qualsiasi tipo, esplicita o implicita, comprese, a titolo esemplificativo, le garanzie implicite e le condizioni di commerciabilità, di idoneità ad uno scopo particolare e di non violazione di diritti altrui; Quantec non garantisce che i Servizi e le funzioni del Software siano idonei a soddisfare le esigenze e le aspettative dell'Utente, né che i Servizi siano privi di interruzioni, né che siano in assoluto puntuali, sicuri o senza errori;
2. Quantec non garantisce che il Software sia compatibile o che funzioni con applicazioni, servizi o software di terze parti e che i servizi continueranno ad essere disponibili e, in caso di interferenza con il funzionamento di software di terze parti, Quantec si riserva il diritto di valutare di volta in volta l'eventuale modifica da apportare al proprio software, valutarne i tempi e modi di applicazione e comunque decidere discrezionalmente se apportarla o meno;
3. qualsiasi materiale scaricato o altrimenti ottenuto tramite l'utilizzo dei Servizi è a rischio e discrezione dell'Utente, che sarà l'unico responsabile per eventuali danni ai propri sistemi informatici o ad altri dispositivi, così come per la perdita di dati risultante dal download di tali materiali;
4. l'Utente riconosce, assumendosene in via esclusiva le relative responsabilità, che l'utilizzo di IndependenceKey e dei Servizi non è adatto a situazioni o ambienti in cui il malfunzionamento, eventuali ritardi, errori o imprecisioni del contenuto, dei dati o delle informazioni fornite dal Prodotto e dai Servizi potrebbero causare morte, danni fisici o ambientali, ivi compresi, a titolo esemplificativo ma non esaustivo, le situazioni in cui vengono utilizzate attrezzature nucleari, strumentazioni di volo o di comunicazione con aeroplani e sistemi relativi al controllo del traffico aereo, di soccorso o di armamento, ivi inclusi gli utilizzi in ambito militare. Per tali applicazioni, Quantec rende disponibile una versione specifica di IndependenceKey;
5. qualsiasi informazione o consiglio, sia orale che scritto, ottenuto dall'Utente da Quantec o dai suoi rappresentanti autorizzati, non potrà in nessun caso essere inteso alla stregua di garanzia da parte di Quantec. In caso di difetti del Software o dei Servizi, i costi derivanti da interventi, correzioni e riparazioni che dovessero rendersi necessari saranno totalmente a carico dell'Utente.
6. Le limitazioni di cui al presente paragrafo s'intendono valide ed efficaci nei limiti di compatibilità con la legge applicabile, come meglio specificato nel paragrafo 11 che segue.

10. LIMITAZIONI DELLA RESPONSABILITÀ

Nei limiti consentiti dalla legge applicabile, Quantec è sollevata da ogni responsabilità per qualsiasi lesione personale o per qualsiasi danno, diretto o indiretto e di ogni genere e specie, inclusi, a titolo esemplificativo ma non esaustivo, i danni per mancato guadagno, interruzione dell'attività, perdita di dati o danneggiamento, errore nella trasmissione o ricezione dei dati, o altri danni o perdite commerciali, derivanti da o correlati a: (i) interruzione delle operazioni del Software per mancanza di energia elettrica oppure per rimozione forzata del dispositivo IndependenceKey dal computer o di un dispositivo di memoria di mass storage connesso nella porta posteriore di IndependenceKey mentre questi era attivo ovvero senza aver prima effettuato l'apposita procedura di "unmount" tramite il Software, (ii) utilizzo o cattivo utilizzo del Software, dei servizi o di qualunque software o applicazione di terze parti congiuntamente al Software o (iii) qualsiasi altro aspetto correlato ai Servizi.

In nessun caso il limite di responsabilità a carico di Quantec nei confronti dell'Utente supererà l'importo di cinque franchi svizzeri (CHF 5.-) per la globalità del danno.

La qui descritta limitazione di responsabilità di Quantec vale indipendentemente dalla causa dei danni e dall'origine della responsabilità (interruzione del contratto, atto illecito o altri) ed anche nel caso in cui Quantec sia stata avvertita della possibilità di tali danni.

Le limitazioni di cui al presente paragrafo s'intendono valide ed efficaci nei limiti di compatibilità con la legge applicabile, come meglio specificato nel paragrafo 11 che segue.

11. ESCLUSIONI

Alcune giurisdizioni non ammettono l'esclusione di determinate garanzie o condizioni o la limitazione o l'esclusione della responsabilità per lesioni personali, perdita o danni causati da negligenza, violazione del contratto o violazione dei termini impliciti o per danni incidentali o consequenziali. Pertanto, le limitazioni di cui ai precedenti paragrafi 9 e 10 s'intendono applicabili solo nei limiti in cui non siano vietate dalle leggi di volta in volta applicabili in base alla giurisdizione dell'Utente e/o del luogo di utilizzo del Prodotto.

ESPORTAZIONE CONTROLLATA

Non è consentito utilizzare, esportare o riesportare il Prodotto se non in conformità con le leggi degli Stati Uniti d'America o del paese in cui il Prodotto è stato acquistato. In particolare, ma senza limitazioni, non è possibile acquistare, esportare o riesportare il prodotto:

1) in nessun paese sottoposto ad embargo da parte degli Stati Uniti,

2) a chiunque figuri nell'elenco del Dipartimento del Tesoro degli Stati Uniti denominato Specially Designated Nationals o negli elenchi del Dipartimento del Commercio degli Stati Uniti denominati Denied Person List o Entity List (Informazioni dettagliate su <http://www.bis.doc.gov/entities/entitylistfaq.html>).

Utilizzando il Prodotto, l'Utente afferma espressamente e garantisce di non figurare negli elenchi di cui sopra e di non trovarsi in uno di tali paesi. L'Utente accetta, inoltre, di non utilizzare il Software per nessuno degli scopi vietati dalla legge, inclusi, a titolo esemplificativo ma non esaustivo, lo sviluppo, la progettazione, la fabbricazione o produzione di armi, armi nucleari, chimiche, biologiche o missili.

ALTRI DIRITTI

I diritti non pubblicati sono protetti dalla Legge Federale Svizzera sul diritto d'autore, reperibile all'indirizzo http://www.admin.ch/ch/i/rs/231_1/index.html.

LEGGE REGOLATRICE ED EVENTUALE NULLITÀ DI UNA O PIÙ CLAUSOLE

Termini e Condizioni della Licenza sono soggette alla legislazione della Confederazione Svizzera e andranno applicate e interpretate in conformità a quest'ultima.

L'eventuale inapplicabilità e/o invalidità e/o inefficacia di una o più clausole o parti di clausole dei Termini e Condizioni della Licenza non comporta l'inapplicabilità e/o invalidità e/o inefficacia delle altre clausole o parti di clausole, le quali, pienamente valide ed efficaci, continueranno ad essere oggetto di applicazione.

INTEGRITÀ DELL'ACCORDO

La Licenza sostituisce ogni eventuale accordo precedente e costituisce l'intero accordo tra l'Utente e Quantec in relazione all'utilizzo del Software e dei Servizi. Eventuali emendamenti o modifiche saranno validi ed efficaci solo se risultanti in forma scritta e sottoscritti da un rappresentante autorizzato di Quantec.

Ogni traduzione della presente Licenza è offerta unicamente per cortesia e non ha valore legale.

Qualora la versione italiana della Licenza e la versione tradotta fossero discrepanti, dovrà ritenersi prevalente la versione italiana, seppur nei limiti di quanto consentito dalla legislazione locale della giurisdizione dell'Utente e/o del luogo di utilizzazione del Prodotto.

Copyright ©2012 Quantec SA. Tutti i diritti riservati.

Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, TI.

Aggiornato in data 05/03/2013

Per ulteriori informazioni, contattare info@quanteclab.com

Garanzia hardware

GARANZIA

Questa Garanzia conferisce all'Utente specifici diritti, oltre a quelli eventualmente attribuitigli dalle leggi del proprio stato (o paese, o regione) e non esclude, limita o sospende alcun diritto degli Utente; inclusi quelli che possono derivare da una non-conformità al contratto di vendita. Invitiamo l'Utente a consultare la normativa del proprio paese, regione o stato.

Limitazioni

Nel limiti previsti dalla legge, questa Garanzia ed i rimedi indicati si intendono esclusivi e sostituiscono qualsiasi altra garanzia, rimedio e condizione, espressa, implicita, verbale, scritta, o legale. Quantec nega specificamente qualsiasi Garanzia di legge, ivi comprese, a titolo esemplificativo, le garanzie di commerciabilità e idoneità a scopi specifici e per vizi occulti o latenti. Qualora le leggi non consentano a Quantec di negare le suddette garanzie, Quantec limita la durata e i rimedi previsti da tale Garanzia al periodo di durata della presente e, a propria discrezione, al servizio di riparazione e sostituzione. In quei paesi, stati e regioni che non ammettono limitazioni sulla durata delle garanzie o condizioni implicite, le limitazioni qui menzionate potrebbero non applicarsi.

Copertura

Quantec garantisce che i prodotti hardware ed accessori contenuti nella confezione originale ("Prodotti Quantec") sono esenti da difetti dei materiali e di produzione per due (2) anni dalla data d'acquisto da parte dell'utente finale ("Periodo di Garanzia") qualora utilizzati in conformità alle linee guida fornite da Quantec. Le linee guida includono a titolo esemplificativo le informazioni contenute nel manuale d'uso, nelle specifiche tecniche, nel sito web e nelle comunicazioni di servizio.

Copertura NON garantita

Quantec non garantisce che l'operatività del prodotto sia esente da interruzioni o errori. Quantec non è responsabile dei danni causati dalla mancata osservanza delle istruzioni d'uso del prodotto. Per maggiori informazioni sui diritti dell'Utente circa l'uso del software si prega di leggere di Licenza del Software Quantec.

La presente Garanzia non si applica a:

- 1) componenti consumabili, come i rivestimenti protettivi soggetti a riduzione nel tempo, a meno che il problema sia stato causato da un difetto di fabbricazione o di manodopera;
- 2) danni causati dall'uso in associazione a prodotti che non siano Quantec;
- 3) un prodotto il cui numero di serie sia stato rimosso o reso illeggibile;
- 4) danni causati da interventi (ivi compresi gli interventi di miglioramento ed upgrade) effettuati da qualunque soggetto che non sia un rappresentante di Quantec o un suo fornitore di servizi di assistenza autorizzato;
- 5) un prodotto che sia stato modificato per alterarne le funzionalità o capacità senza il consenso scritto di Quantec;
- 6) danni causati da incidenti, abuso, uso improprio, contatto con liquidi, incendio, terremoto od altra causa esterna;
- 7) danni causati dall'utilizzo del prodotto in modo non conforme con gli usi previsti o descritti da Quantec;
- 8) danni estetici, ivi inclusi, a titolo esemplificativo e non esaustivo, graffi, ammaccature su tutte le superfici sia in metallo che in plastica;
- 9) difetti riconducibili alla ordinaria usura del prodotto o altrimenti dovuti al normale invecchiamento dello stesso.

Importanti limitazioni

Quantec si riserva il diritto di limitare il servizio di Garanzia nel paese nel quale Quantec o i suoi distributori autorizzati hanno venduto originariamente il prodotto.

Responsabilità dell'Utente.

Il dispositivo crittografico portatile IndependenceKey (d'ora in avanti "IKEY") è un apparato elettronico progettato per applicazioni nel solo ambito consumer. L'Utente deve prestare attenzione a quanto descritto nel manuale di istruzioni ed evitare di collegare alla presa USB presente sul retro del prodotto dispositivi non conformi USB e non rientranti nelle specifiche funzionali del prodotto IKEY. IKEY consente di collegare, a tale porta USB posteriore, comuni "chiavette" USB di data storage flash, Hard Disk USB solo se alimentati esternamente tramite il proprio alimentatore, tastiere USB, mouse USB e tutti gli accessori della linea IKEY, tra cui il dispositivo "Security Cap", il "Data Bank" e specifiche cuffie USB digitali (headset USB).

Il dispositivo "Security Cap" consente di recuperare le informazioni in caso amnesia ovvero in caso di perdita, furto o non funzionamento del dispositivo principale IKEY. Si raccomanda pertanto di effettuare regolarmente i back-up nel Security Cap come espressamente indicato nel manuale di istruzioni ricevuto insieme al prodotto oppure di utilizzare, quando disponibile, il servizio opzionale di backup automatico Data Bank.

Prima di erogare il servizio di Garanzia, potrebbe essere richiesto di fornire la prova d'acquisto, di rispondere a domande dirette all'assistenza con diagnosi di possibili problematiche e di seguire determinate procedure per ottenere il servizio di Garanzia. Prima di consegnare il prodotto al servizio di Garanzia l'utente deve: contattare il centro assistenza per individuare la natura del problema della IKEY o del Security CAP e solo allora procedere con la spedizione del prodotto secondo le istruzioni ricevute.

IKEY contiene al proprio interno, in forma crittografata e non accessibile senza la Master Password dell'Utente, tutti gli elementi di identificazione dell'Utente, le chiavi crittografiche generate durante l'uso del dispositivo stesso e le associazioni con altri utenti nonché i dati relativi al Password Manager (dati di accesso a siti web, servizi di terzi, posta elettronica, homebanking e così via). La versione dotata anche di mass storage interna, contiene anche il relativo storage, anch'esso totalmente crittato, come un tradizionale dispositivo USB data flash.

A seguito del servizio di riparazione, il prodotto o un prodotto sostitutivo sarà restituito all'Utente, qualora possibile, con i dati dell'Utente, ovvero nella configurazione in cui è stato acquistato il prodotto originale, opportunamente aggiornato e privo dei dati dell'Utente. In tal caso Quantec e i suoi incaricati non sono responsabili per eventuali danni o perdita di programmi software, dati, files o altre informazioni contenute su tale supporto o di qualsiasi componente del prodotto oggetto del servizio di questa Garanzia. L'Utente sarà tenuto ad effettuare il ripristino dei propri dati. In tal caso, il prodotto restituito all'Utente privo dei dati originali dell'Utente stesso potrà essere ripristinato tramite le apposite procedure previste dal prodotto tramite il proprio dispositivo di back-up "Security Cap", seguendo le procedure previste per il prodotto.

In tal caso, ovvero quando il contenuto del dispositivo Quantec vada perso o possa essere riformattato/resettato durante il servizio di Garanzia, per ripristinare tale contenuto l'Utente deve disporre del dispositivo di back-up Security Cap nel caso di malfunzionamenti nella IKEY, oppure della propria IKEY nel caso di malfunzionamenti del Security Cap. In mancanza di entrambi, Quantec non può garantire per nessun motivo il ripristino dei dati persi, ovvero dei dati di identificazione dell'Utente, delle chiavi crittografiche generate durante l'uso del dispositivo stesso e le associazioni con altri utenti nonché dei dati relativi al Password Manager. In aggiunta, l'Utente può comunque sottoscrivere il servizio on-line di "Data Bank" e, pertanto, tramite il proprio dispositivo di back-up "Data Bank" effettuare il ripristino. Tale servizio è opzionale e non rientra nella fornitura standard di IKEY.

Il recupero ed il ripristino dei dati all'interno della propria IKEY da parte dell'Utente sono a carico dell'Utente stesso e non sono coperti dalla presente Garanzia. Si precisa che l'eventuale impossibilità, da parte dell'Utente, di poter ripristinare tali dati, ovvero la mancanza del dispositivo Security Cap in caso di ripristino in garanzia della propria IKEY o la mancanza della propria IKEY nel caso di ripristino in garanzia del proprio Security Cap oververla mancanza di entrambi i dispositivi di proprietà dell'Utente rende impossibile recuperare i dati dell'Utente stesso, ovvero le chiavi crittografiche, i dati di associazione con altri utenti ed i dati del Password Manager con relativa impossibilità di accedere ai file, cartelle e dischi già crittografati in precedenza. In tal senso, si raccomanda sempre all'Utente di riportare il proprio Security Cap in un luogo sicuro ed a lui solo accessibile, con temperatura preferibile tra gli 0°C ed i 30°C ed umidità controllata. In aggiunta, l'Utente può utilizzare il servizio di back-up automatico e continuativo on-line, tramite il proprio "Data Bank" (opzionale), avendo la possibilità di disporre di un terzo dispositivo atto a recuperare i sopracitati dati nel caso di perdita, rottura o ripristino in garanzia sia della propria IKEY che del proprio Security Cap.

Importante: non tentare di aprire il prodotto e/o di dissaldarne componenti. Il tentativo di apertura causa danni che non sono coperti dalla presente Garanzia. Solo Quantec o un componente dello staff di assistenza possono prestare i servizi su tale prodotto. L'apertura non autorizzata determina la cessazione immediata della garanzia.

Garanzia

In caso di valida richiesta ricevuta entro il periodo di Garanzia, Quantec potrà, a propria discrezione

- 1) riparare il prodotto utilizzando componenti nuovi o componenti ricondizionati equivalenti al nuovo per prestazioni e affidabilità,
- 2) sostituire il prodotto con un prodotto che abbia funzionalità minime equivalente al prodotto e sia costituito da parti nuove o usate che abbiano le medesime prestazioni e affidabilità di un prodotto nuovo,
- 3) rimborsare il prezzo d'acquisto del prodotto (escluse le originarie spese di spedizione ed eventuali dazi) a fronte della restituzione dello stesso.

Quantec garantisce i prodotti per due (2) anni.

Le parti sostituite, saranno garantite per il periodo più lungo tra il periodo residuo della Garanzia del prodotto e un (1) anno dalla data di sostituzione o riparazione. Dopo la sostituzione, il prodotto o componente sostitutivo si intendono di proprietà dell'Utente e il prodotto o componente sostituito si intende di proprietà di Quantec.

Servizio di Garanzia

- Prima di richiedere il servizio di Garanzia si invita l'Utente a consultare le risorse di assistenza online (FAQ, FORUM, BLOG) presso il sito www.independencekey.com. Nel caso in cui il prodotto continui a non funzionare correttamente anche dopo aver seguito le istruzioni indicate nelle risorse di assistenza online, l'Utente potrà contattare Quantec secondo le informazioni fornite qui di seguito. Il rappresentante Quantec e/o il supporto tecnico Quantec supporterà l'Utente al fine di appurare se il prodotto necessita del servizio di assistenza e, in tal caso, illustrerà le modalità di prestazione del servizio garanzia da parte di Quantec. Quantec presterà il servizio di Garanzia attraverso una o più delle seguenti modalità: Acquisto presso rivenditore autorizzato. L'Utente potrà consegnare il prodotto ad un rivenditore Quantec. Alorché l'Utente avrà ricevuto la comunicazione di completamento del servizio, lo stesso sarà tenuto al tempestivo ritiro del prodotto presso il rivenditore. Le eventuali spese di trasporto saranno a carico dell'Utente.
- Acquisto on-line. L'Utente potrà inviare il prodotto alla sede Quantec, a proprie spese. Al completamento del servizio, Quantec invierà il prodotto all'Utente facendosi carico delle spese di spedizione e dandone immediata comunicazione all'Utente stesso.

Quantec si riserva il diritto di modificare le modalità di prestazione del servizio di Garanzia nei confronti dell'Utente, nonché la disponibilità di particolari tipologie di servizio per il prodotto. Le tipologie di servizio saranno limitate alle opzioni disponibili a seconda del paese da cui provverrà la richiesta del servizio di Garanzia. Le opzioni di servizio, la disponibilità delle parti e i tempi di riscontro possono variare da paese a paese. Se il prodotto non può essere riparato o sostituito nel paese in cui si trova, l'Utente dovrà farsi carico dei costi di spedizione e gestione del servizio. Se il servizio di Garanzia viene richiesto in un paese diverso da quello in cui il prodotto è stato acquistato, l'Utente è tenuto ad osservare le leggi e i regolamenti applicabili in materia di importazione ed esportazione, a farsi carico dei dazi doganali, dell'IVA e di tutte le altre imposte ed oneri associati. In caso di fornitura del servizio di Garanzia internazionale, Quantec potrà riparare o sostituire i prodotti e i componenti difettosi con prodotti e componenti equiparabili che siano conformi alle normative locali.

Limitazioni di responsabilità

Fatta eccezione per quanto previsto dalla presente Garanzia e fino al limite massimo previsto dalla legge, Quantec non è responsabile per danni diretti, speciali, indiretti o accessori derivanti dalla violazione della Garanzia o di sue disposizioni, compresi quelli previsti da qualsiasi altro principio di legge, compresi, a solo titolo esemplificativo, danni all'immagine; perdita, danni, alterazione o distruzione di dati; la perdita di utilizzo, perdita di fatturato, perdita di utili effettivi o contrattuali previsti; perdita di liquidità; perdita di risparmi attesi; perdita di affari; perdita di opportunità; perdita di avviamento; o qualsiasi perdita o danno indiretto o accessorio a prescindere dalla causa, ivi compresa la sostituzione di attrezzature e beni, le spese di recupero dati, riprogrammazione o riproduzione dei programmi o dei dati contenuti o utilizzati con il prodotto.

Quantec non garantisce specificamente che sarà in grado di riparare o di sostituire ogni prodotto coperto dalla presente Garanzia senza rischio o perdita di programmi o dati memorizzati nel prodotto ivi inclusi i dati identificativi dell'Utente stesso, le chiavi crittografiche, i dati di associazione con altri utenti ed i dati del Password Manager né potrà esserle addebitata la perdita di qualsiasi tipo di dato, informazione, file ivi contenuto o l'impossibilità in tali casi di poter accedere a dati, file, cartelle e dischi già crittografati in precedenza tramite IKEY.

Le summenzionate limitazioni ed esclusioni potrebbero non essere applicabili in quei paesi, regioni e province che non ammettono l'esclusione o la limitazione in caso di danni accidentali o consequenziali.

Privacy

Quantec si impegna a conservare ed utilizzare le informazioni sulla clientela in conformità alle Norme sulla Privacy, reperibili alla pagina <http://www.independencekey.com/blog/privacy/>.

I rivenditori, agenti o dipendenti di Quantec non sono autorizzati ad apportare modifiche, estensioni o integrazioni alla presente Garanzia. Nel caso in cui alcune delle condizioni della presente Garanzia siano dichiarate invalide, nulle o non applicabili, tutte le restanti condizioni saranno pienamente valide ed efficaci. La presente Garanzia è regolata dalla legge del luogo di acquisto del prodotto e sulla base di quest'ultima dovrà essere interpretata.

Quantec o i suoi aventi causa sono i prestatori di Garanzia sulla base della presente Garanzia.

Copyright ©2012 Quantec SA. Tutti i diritti riservati.

Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, TI.

Aggiornato in data 05/03/2013

Per ulteriori informazioni, contattare info@quantecclub.com

Norme sulla Privacy

NORME SULLA PRIVACY

Le Norme sulla Privacy disciplinano le modalità e i limiti di raccolta, utilizzo, conservazione, divulgazione, trasferimento e memorizzazione dei dati da parte di Quantec e chiariscono gli strumenti a disposizione dell'utente dei servizi Quantec (l'“**Utente**” e/o gli “**Utenti**”) per la tutela e la protezione della propria privacy.

Invitiamo gli Utenti a leggere con attenzione il presente documento e a contattare Quantec in caso di eventuali domande.

1.PREMESSE

Quantec **non è in condizione di rilevare in alcun modo le chiavi di crittografia né di accedere ai dati crittografati dell'utente**. Pertanto:

1. L'Utente è responsabile in via esclusiva del materiale che sottopone a crittografia e dovrà farlo nel rispetto delle leggi del proprio paese. Quantec memorizza nei propri server, all'atto dell'accesso dell'Utente, data e ora di accesso, indirizzo IP dell'Utente e dati geografici correlati. Per i [servizi di accounting](#) dell'Utente sui siti web e di assistenza (trouble ticketing) Quantec memorizza l'account dell'Utente ed i relativi dati opzionali forniti all'esclusivo scopo di garantire l'accesso sicuro e protetto alle aree riservate ed ai servizi di assistenza.
2. Qualora l'Utente utilizzi i [servizi avanzati Quantec](#) (ad esempio, file transfer sicuro o connessioni in streaming con altri utenti), Quantec sarà a conoscenza del mero concretizzarsi della condivisione di informazioni tra Utenti individuati (conoscenza necessaria alla fornitura dei servizi avanzati); tipologia e contenuto delle informazioni condivise rimarranno invece del tutto sconosciuti a Quantec.
3. Ogni eventuale file e/o insieme di dati in transito attraverso i server Quantec è criptato con le chiavi crittografiche dell'Utente (le “Chiavi”), che l'Utente gestisce in via esclusiva. Le Chiavi risiedono nel dispositivo IndependenceKey dell'Utente, sbloccabile unicamente (i) tramite connessione del Security Cap cui il dispositivo è univocamente associato o (ii) con la Master Password a conoscenza esclusiva dell'Utente.
4. I dati opzionali di cui al punto 2 e quanto specificato nel punto 3 costituiscono le sole informazioni nella disponibilità di Quantec, che Quantec potrà pertanto rendere note in caso di ordine, ingiunzione o richiesta da parte di qualsivoglia autorità pubblica o governativa competente. Quantec non sarà in condizione, in nessun modo, di rendere nota la tipologia ed il contenuto delle informazioni che gli utenti possono scambiare, direttamente e/o per tramite dei propri server, perché crittografate alla fonte tramite l'applicazione delle chiavi crittografiche esclusivamente note agli utenti stessi. Quantec, se non espressamente necessario per erogare i servizi avanzati, non memorizza e conserva i dati in transito, se non per il tempo minimo necessario; in nessun caso Quantec memorizza e conserva dati in transito in relazione ai servizi in streaming real-time come i servizi VoIP.

2.DATI RACCOLTI

Tipologia dei dati raccolti da Quantec:

Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, (tramite i dati medesimi o) anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (ad esempio nome e cognome);

Dati non personali o anonimi: dati non riconducibili univocamente ad un determinato soggetto e pertanto inadatti a consentirne, sia direttamente che indirettamente, l'identificazione (vi rientrano i c.d. dati aggregati: dati che raggruppano in massa informazioni relative a più Utenti, con una finalità statistico/commerciale: ad esempio rilevazioni dei siti web e dei prodotti Quantec di maggiore interesse per l'Utente).

2.A Modalità di raccolta dati

La raccolta dei dati (personali e non) dell'Utente da parte di Quantec ha lo scopo di migliorare i prodotti ed i servizi offerti all'Utente da Quantec. A tale scopo, Quantec si riserva la facoltà di combinare i dati personali raccolti con altri dati.

Modalità di raccolta dati:

a) Dati personali forniti dall'Utente

Entrando in contatto con Quantec, all'Utente può essere richiesto di fornire i propri dati personali: l'acquisto di prodotti e l'utilizzo di servizi Quantec può richiedere all'Utente la creazione di un account. Durante la creazione dell'account, l'Utente potrà essere chiamato a fornire alcuni dati personali, quali nome e cognome, indirizzo email, numero di telefono (opzionale) e partita iva in caso di Utente aziendale.

b) Dati personali raccolti dall'utilizzo dei servizi Quantec da parte dell'Utente

Con l'attivazione e l'uso di IndependenceKey, lo scaricamento degli Aggiornamenti software, l'ingresso al forum sui siti web di prodotto, Quantec raccoglierà:

- (i) il nickname dell'utente, il suo alias, il numero di serie del prodotto, il numero di serie identificativo dell'utente e gli eventuali ulteriori dati opzionali che l'utente avrà inserito nel software di gestione in dotazione con il prodotto (nome, cognome, email, azienda, sito web, etc..),
- (ii) e i dati informativi della macchina in cui è installato il software (ad esempio, tipo di microprocessore e velocità, risoluzione dello schermo, tipo di sistema operativo installato, quantità di memoria RAM disponibile per le applicazioni e capacità dei dischi).

c) Dati non personali raccolti dall'utilizzo dei servizi Quantec da parte dell'Utente

Quantec può raccogliere informazioni sui servizi utilizzati dall'Utente e sulle relative modalità di utilizzo. Ad esempio, Quantec potrà raccogliere dati riguardanti l'attività degli Utenti sul sito web Quantec, i forum e l'IKey Store, o le attività registrate da altri prodotti e servizi Quantec.

2.B Finalità e modalità di utilizzo dei dati raccolti

Quantec utilizza i dati raccolti nei termini di cui al punto 2A che precede:

- 1) per garantire un costante aggiornamento dell'Utente, ad esempio sugli ultimi prodotti Quantec, sugli aggiornamenti software e su eventuali eventi promossi da Quantec;
- 2) con finalità di marketing: strategia commerciale e pubblicitaria;
- 3) per comunicazioni relative al rapporto contrattuale con l'Utente: ad esempio comunicazioni relative all'acquisto di prodotti e ad eventuali modifiche dei termini e condizioni di licenza Quantec.
- 4) per incrementare la rispondenza dei prodotti e servizi Quantec alle esigenze ed aspettative dell'Utente, anche in termini di assistenza e di contenuti web;
- 5) per finalità interne di analisi, verifiche e ricerche, con l'obiettivo di un costante up-grade qualitativo dei prodotti e dei servizi Quantec. Si ribadisce che Quantec non ha modo alcuno di rilevare le chiavi di crittografia, né può aprire i file, cartelle e dischi crittografati da IKEY. I dati raccolti in sede di analisi e ricerca si limitano pertanto alle performance del dispositivo.

Cookie e altri identificatori anonimi

Il sito web, i servizi online, le applicazioni interattive, i messaggi email e le pubblicità di Quantec potrebbero avvalersi di “cookie” o altri identificatori anonimi (ad esempio pixel tag e web beacon) per raccogliere e memorizzare informazioni relative all'accesso e/o utilizzo dei servizi e siti web Quantec da parte dell'Utente.

Come accade nella maggior parte dei siti web, alcuni dati vengono raccolti automaticamente ed archiviati in log files. Tali dati includono gli indirizzi Internet Protocol (IP), il tipo e la lingua del browser, l'Internet Service Provider (ISP), pagine di entrata/uscita, sistema operativo, data, ora e dati del clickstream.

I dati raccolti tramite i cookie o altri identificatori anonimi aiutano a comprendere il comportamento, le tendenze, le aspettative ed il target degli Utenti, consentono di rilevare le parti di sito maggiormente visitate ed i servizi più utilizzati e permettono di saggiare l'efficacia delle strategie pubblicitarie e di marketing adottate. Tramite tali dati è possibile migliorare e "personalizzare" l'esperienza Quantec di ogni Utente (ad esempio, qualora un Utente salvasse le preferenze della lingua, sarebbe possibile visualizzare i servizi nella lingua preferita dell'Utente), nonché di incrementare la qualità generale dei servizi Quantec.

I dati raccolti attraverso i cookie o altri identificatori anonimi sono trattati come dati non personali. Ciononostante, nella misura in cui indirizzi Internet Protocol (IP) o identificatori simili siano considerati dati personali dalla legge locale, tali identificatori saranno trattati alla stregua di dati personali. Analogamente, nella misura in cui dati non personali siano aggregati con dati personali, i dati così aggregati saranno trattati come dati personali.

2.C Accesso ai dati personali e aggiornamento

Quando l'Utente utilizza i servizi Quantec è messo in condizione di accedere ai suoi dati personali. Ove i dati non fossero corretti, su segnalazione dell'Utente, Quantec ne consentirà l'aggiornamento o l'eliminazione, salvo che debba conservarli per legittime finalità commerciali o legali. In caso di aggiornamento dei dati personali, all'Utente potrà essere previamente richiesto di confermare la propria identità.

Quantec si riserva la facoltà di rifiutare eventuali richieste di aggiornamento e/o eliminazione dei dati raccolti, laddove tali richieste richiedano un impegno tecnico eccessivamente gravoso e/o sproporzionato (ad esempio lo sviluppo di un nuovo sistema o la modifica sostanziale di una prassi esistente), mettano a rischio la privacy di altre persone, ovvero risultino concretamente inattuabili (ad esempio richieste relative a informazioni memorizzate su dispositivi di backup).

Al fine di evitare eventuali distruzioni dolose o accidentali dei dati, una volta che l'Utente abbia deciso di eliminare i propri dati dai servizi Quantec, Quantec potrà non eliminare subito le copie rimanenti dai server attivi e potrà non rimuovere le informazioni dai sistemi di backup.

2.D Divulgazione dei dati raccolti

Quantec non fornisce i dati personali dell'Utente, senza il suo consenso, a società, organizzazioni o persone terze, salvo le eccezioni che seguono:

(i) Quantec condivide i dati personali con le società che eseguono gli ordini degli Utenti, consegnano i prodotti e forniscono assistenza logistica. Queste società possono essere ubicate ovunque operi Quantec e sono obbligate a proteggere i dati personali dell'Utente nei termini di cui alla presente policy, con la massima cura e diligenza;

(ii) per legge, procedimento giudiziario, contenzioso, e/o richieste da parte di autorità pubbliche e governative all'interno o al di fuori del paese di residenza, ragioni di sicurezza nazionale, rispetto della legge o altre questioni di importanza pubblica, Quantec potrebbe dover divulgare il numero di serie del prodotto utilizzato da un dato Utente e l'eventuale storia disponibile delle connessioni con altri Utenti. Nessun altro dato potrà essere divulgato da Quantec nelle qui descritte circostanze. Come detto, eventuali file e dati in transito attraverso i server Quantec non possono essere decifrati se non attraverso il dispositivo IKEY e la relativa Master Password e/o Security Cap, che rimangono nel possesso e a disposizione esclusiva dell'Utente. Le informazioni eventualmente divulgate da Quantec nei casi qui indicati non sono pertanto, in nessun caso, idonee a consentire l'accesso alle chiavi di crittografia, né permettono di decrittografare i dati dell'Utente.

(iii) in caso di ristrutturazione, fusione o vendita, Quantec si riserva il diritto di trasferire a terzi tutti i dati raccolti.

2.E Protezione dei dati raccolti

Quantec prende precauzioni, misure tecniche, fisiche ed amministrative, adottate con la normale diligenza professionale, al fine di proteggere i dati personali da perdita, furto e abuso, nonché da accesso non autorizzato, rivelazione, alterazione e distruzione.

I servizi online di Quantec come l'IKey Store utilizzano sistemi di crittazione Secure Sockets Layer (SSL) su tutte le pagine web in cui vengono raccolti dati personali. Per eseguire acquisti attraverso tali servizi, l'Utente è invitato ad utilizzare un browser abilitato SSL come Safari, Firefox o Internet Explorer, per una maggiore riservatezza dei dati personali trasmessi via Internet.

ATTENZIONE: utilizzando alcuni prodotti, servizi o applicazioni, pubblicando su un forum, chat room o servizio di social network Quantec, i dati personali condivisi sono visibili agli altri Utenti e possono essere da loro letti, raccolti o utilizzati. In tali occasioni l'Utente è solo ed unico responsabile dei dati personali che sceglie di inoltrare.

I servizi erogati dai server Quantec sono soggetti ad autenticazione e crittografia hardware del canale, ottenuta direttamente tramite il dispositivo IndependenceKey ed i server stessi. Le comunicazioni sono, pertanto, tutte criptate ed i dati stessi vengono conservati nel datacenter Quantec in un'apposita struttura fisicamente dislocata nel territorio Svizzero, blindata e protetta in appositi locali dotati di autenticazione biometrica. La connessione telematica verso tali server è, pertanto, gestita direttamente tra i server stessi ed il dispositivo IndependenceKey per tramite del computer host nel quale il dispositivo medesimo è inserito. Pertanto, tutte le comunicazioni tra IndependenceKey ed i server sono crittografate a livello hardware, comunicazioni atte ad erogare i servizi di prima connessione ed attivazione, associazione remota tra utenti, scambio file e telefonia VoIP tramite i servizi avanzati Quantec. Si ribadisce che i server Quantec non possono altresì mai entrare nel merito del contenuto dei file, dei dati e dei flussi VoIP in streaming scambiati tra gli utenti perché, a loro volta, crittografati all'origine con chiavi crittografiche univoche note solo ai dispositivi IndependenceKey degli utenti stessi.

2.F Conservazione dei dati raccolti

Quantec conserva i dati personali in modo accurato, completo e aggiornato per il tempo necessario a perseguire le finalità dei servizi erogati secondo le presenti Norme sulla Privacy, a meno che un periodo di conservazione più lungo sia richiesto o permesso dalla Legge.

3. ESCLUSIONI

Minori

Quantec non raccoglie dati personali da e/o relativi a persone di età inferiore a 13 anni. Nel caso in cui tale circostanza si dovesse verificare, Quantec procederà all'immediata eliminazione di tali dati, non appena a conoscenza.

Siti e servizi di terzi

I siti Internet, prodotti, applicazioni e servizi Quantec possono contenere link a siti Internet, prodotti e servizi di terzi, cui la presente Policy non è applicabile. Si invita pertanto l'Utente a consultare i regolamenti privacy di tali terzi fornitori.

4. MODIFICHE

Le Norme sulla Privacy di cui al presente documento potrebbero essere soggette a modifiche occasionali. Quantec si impegna ad ogni modo a non ridurre i diritti degli Utenti senza il loro esplicito consenso. Eventuali modifiche alle presenti Norme sulla Privacy saranno pubblicate in questa pagina. Le versioni precedenti delle Norme sulla privacy saranno archiviate e rimarranno in ogni momento consultabili dall'Utente.

Copyright ©2012 Quantec SA. Tutti i diritti riservati.
Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, TI.

Aggiornato in data 05/03/2013

Per ulteriori informazioni, contattare info@quantecclub.com

Compatibile Microsoft Windows XP SP3, Windows Vista 32 e 64 bit, Windows 7 32 e 64 bit.



Norme e riferimenti tecnici: EN 55022, EN 61000-4-2, EN 61000-4-4, EN 61000-4-6. FCC PART 15 SUBPART B CLASS B



Copyright © Quantec SA 2013
IndependenceKey™ is a Trademark of Quantec SA
International PCT Patent Pending

Brevetti depositati in Svizzera con procedura di estensione internazionale PCT
in 138 Paesi nr. 0021212 del 17/02/2012 e nr. 0075312 del 01/06/2012

QUANTEC

QUANTEC SA
Corso San Gottardo, 86
6830 Chiasso
Switzerland
Telephone: +41.(0) 91.696.16.16
Email: info@quanteclub.com

